The Use of Baselining in Acquisition Program Management

RAND

Jeffrey A. Drezner
Richard A. Krop

National Defense Research Institute

The research described in this report was sponsored by the Office of the Secretary of Defense (OSD). The research was conducted in RAND's National Defense Research Institute, a federally funded research and development center supported by the OSD, the Joint Staff, and the defense agencies under Contract DASW01-95-C-0059.

Library of Congress Cataloging-in-Publication Data

Drezner, Jeffrey A.
The use of baselining in acquisition program management / Jeffrey A. Drezner, Richard A. Krop.
p. cm.
"Prepared for the Office of the Secretary of Defense by RAND's National Defense Research Institute."
"MR-876-OSD."
Includes bibliographical references.
ISBN 0-8330-2550-3
1. United States—Armed Forces—Procurement. I. Krop, Richard A., 1962– . II. United States. Dept. of Defense. Office of the Secretary of Defense. III. National Defense Research Institute (U.S.). IV. Title.
UC263.D7224 1997
355.6' 212—dc21 97-36326
CIP

RAND is a nonprofit institution that helps improve public policy through research and analysis. RAND's publications do not necessarily reflect the opinions or policies of its research sponsors.

Published 1997 by RAND
1700 Main Street, P.O. Box 2138, Santa Monica, CA 90407-2138
1333 H St., N.W., Washington, D.C. 20005-4707
RAND URL: http://www.rand.org/
To order RAND documents or to obtain additional information, contact Distribution Services: Telephone: (310) 451-7002; Fax: (310) 451-6915; Internet: order@rand.org

The Use of Baselining in Acquisition Program Management

Jeffrey A. Drezner

Richard A. Krop

Prepared for the
Office of the Secretary of Defense

MR-876-OSD

National Defense Research Institute

RAND

PREFACE

All major weapon system programs establish a program baseline early in the acquisition cycle which sets forth cost, schedule, and performance targets for the program. If the thresholds are exceeded, a review and assessment procedure is initiated in an attempt to understand why the threshold was "breached" and how the program can be brought back on track. Most programs experience events that require changes to their baselines at some point in their life-cycles. The baselining process can be a useful management tool for acquisition managers by providing metrics for measuring program status and a process for responding to deviations from the plan.

The overall goal of the research reported here is to enhance the usefulness of the acquisition program baselining (APB) process as a management tool for acquisition decisionmakers. This report documents the results of both Phase 1 and Phase 2 research efforts. It should interest analysts and government officials concerned with the defense acquisition process.

This research was sponsored by the Office of the Under Secretary of Defense (Acquisition & Technology) Acquisition Program Integration. The research was performed in the Acquisition and Technology Policy Center of RAND's National Defense Research Institute. The institute is a federally funded research and development center sponsored by the Office of the Secretary of Defense, the Joint Staff, and the defense agencies.

CONTENTS

FIGURES

TABLES

SUMMARY

All major weapon system programs establish an acquisition program baseline (APB) early in the acquisition cycle which sets forth cost, schedule, and performance targets for the program. Associated with the baseline is a set of cost, schedule, and performance thresholds. If these thresholds are exceeded, a review and assessment procedure is initiated in an attempt to understand why the threshold was "breached" and how the program can be brought back on track. Given the uncertainty inherent in complex system development programs, most programs experience events that result in a baseline breach at some point in their life-cycles. These breaches are often resolved by approving changes to the baseline.

Until recently, the baselining process applied a uniform formula to establish thresholds, regardless of the fact that some deviations from the baseline are inherently more important than others. The result was a large number of breached programs which can take significant time to rebaseline and can thus require the attention of senior acquisition managers over an extended period. Recent changes in acquisition legislation, regulations, and directives allow for increased tailoring of the parameters included in the baseline and the thresholds associated with those parameters. However, no criteria for appropriate tailoring have been established. An awareness of the potential relationships between program life-cycles and developmental events, and the factors affecting deviations from the baseline can help acquisition decisionmakers develop appropriately tailored baselines and thresholds.

The goal of this research is to enhance the usefulness of the acquisition program baselining process as a management tool for acquisition decisionmakers. Specifically, we develop an analytic tool that can be used for analysis of historical trends in the number, duration, and factors affecting APB breaches, and analyze the relationship between program acquisition life-cycles and the factors affecting deviations from program baselines.

This research begins to address two broad policy issues. The first concerns how to discriminate among the different types of baseline breaches. Second, within the context of the current initiatives on acquisition reform, how can the APB document and process be used to improve acquisition management. We examine several specific research questions:

- How has the APB process worked in the past? This includes characterizing the process and the baseline breaches, as well as recording actual experience (frequency and type of breaches).
- What factors affect APB breaches? This involves determining the root cause of a breach, if possible, or at least constructing some links in the chain of events leading to the breach.
- To what extent are APB breaches associated with a program's acquisition life-cycle? The interest here is in understanding whether breaches are associated with program events in some way.

Our results provide evidence that most programs experience baseline breaches at least once during their life-cycles—some programs as many as nine. Most of the changes to program baselines are to the cost and schedule portion of the baselines. The majority of the changes are due to real breaches of baseline thresholds, although a sizable share of the changes were revisions that did not breach the threshold. The performance section of the baseline was changed less often; the majority of these changes were revisions to the performance targets, not breaches of the performance thresholds.

Between April 1992 and June 1996, an average of 28 programs were in breach status each month. The overall trend in the number of breaches is downward, driven by a decline in the number of breaches carried-over from one month to the next. Since January 1995, the av-

erage number of programs in breach each month is 14. An average of 25 percent of active major defense acquisition programs were in breach status each month during the same period. The decline in the number of breaches persists even if we take into account the approximately 30 percent decline in the number of active major defense acquisition programs. On average, 12.5 percent of active major defense acquisition programs (MDAPs) were in breach since January 1995, compared to close to 40 percent during 1992.

The average length of time a program spent in breach over this period was just over 9 months. The average length of time tended to decline the later the breach occurred in the period. A significant number of programs were in breach for over 20 months. Consistent with the decline in the average duration of the breaches, fewer programs have been in breach for extended periods more recently than earlier in the period.

Identifying the factors affecting baseline breaches is challenging, given the available data. We developed a taxonomy with two levels. The first level consists of broad issue-oriented categories. The second level is more detailed and reflects actual events and decisions. Unfortunately, data are not systematically collected to support the identification and analysis of root causes. Nevertheless, some interesting observations can be made from the analysis we performed:

- Baseline breaches usually result from a complex chain of events and decisions. At the program level, these events and decisions are unique to each program.
- Multiple factors are common, both in terms of independently causing the same breach or independently causing independent breaches.
- There are no dominant factors at either level of our taxonomy. First-order factors—funding, technical, contractor, requirements, and program redirection related factors—are about evenly distributed, each affecting about 20 percent of the breaches. While some differences emerge at the second-order level, five factors—DoD funding reductions, technical difficulty, quantity changes, revised guidance, and misestimation—are about equally common.

Few relationships were observed between program life-cycle events or program maturity and baseline breaches. There appears to be no time-based pattern to the occurrence of breaches. Similarly, the timing of breaches appears to be generally unrelated to the duration of breaches, the type of parameter that changed, the type of deviation, and the factors affecting the breach. These results suggest that the unique characteristics of programs drive the timing of APB breaches and that because each breach is associated with a unique set of programmatic and environmental factors, the timing of such breaches cannot be predicted with certainty.

We have two related sets of recommendations for enhancing the usefulness of the APB as a management tool.

First, *careful tailoring of the parameters to include in the APB, the thresholds associated with those parameters, and the responses to baseline breaches should be implemented to the full extent possible.* Current regulations allow for, even encourage tailoring both parameters and thresholds to the unique characteristics of the program. We believe that this is an appropriate way to reflect the relative importance and risk in each program. Tailoring has the further advantage of making subsequent breaches equivalent in importance across programs, since thresholds should reflect the risk preferences of decisionmakers and those preferences can be consistently applied across programs. Equivalence may imply high thresholds for low cost, low risk, lower priority programs (resulting in relatively fewer breaches requiring senior management attention) or very low thresholds for high cost, high visibility, high priority programs (resulting in relatively more frequent breaches requiring senior management attention). The critical implementation challenge here is to develop a set of risk-based criteria for establishing parameters to include and the thresholds associated with those parameters that can be consistently applied across programs.

Second, *two important substantive and semantic distinctions should be made among breaches and the causes of those breaches.* For one, breaches should not be interpreted as adversely reflecting the quality of program management. Negative connotations should be removed, thus encouraging faster breach reporting and more thorough documentation of the causes or factors. For another, a distinction should be made between factors that DoD has some ability to influ-

ence, and those that are entirely external to DoD's acquisition management processes. A notional illustration of the relative distribution of internal and external factors affecting breaches suggests that slightly over half of the breaches are caused by factors or events that DoD has some ability to influence. Relatively more attention to these breaches and the factors that cause them would enhance the usefulness of the APB process.

ACKNOWLEDGMENTS

This research would not have been possible without the help of several DoD officials. John Smith and Young Shin provided guidance and access to OSD APB and DAES files. Bob Jordan and Lois Batts provided access to Army and Navy APB process related files. Larry Gwodz provided information and visibility into other aspects of the DAES process. Their assistance is greatly appreciated.

Our RAND colleague, Fred Timson, provided a thoughtful review of the draft document, resulting in a much improved final product.

The authors are responsible for any remaining errors of commission or omission.

Preceding Page Blank

ABBREVIATIONS AND ACRONYMS

ACAT	Acquisition category
APB	Acquisition program baseline
BCR	Baseline change request
CAE	Component acquisition executive
CDR	Critical design review
DAB	Defense Acquisition Board
DAE	Defense acquisition executive
DAES	Defense Acquisition Executive Summary
EMD	Engineering and manufacturing development
FASTA	Federal Acquisition Streamlining Act, 1994
JROC	Joint Requirements Oversight Council
MCS (ATTCS)	Maneuver Control System (Army Tactical Command & Control System)
MDA	Milestone Decision Authority
MDAP	Major defense acquisition program
OIPT	Overarching Integrated Product Team
OSD	Office of the Secretary of Defense

OUSD (A&T) API/ASM	Office of the Under Secretary of Defense (Acquisition and Technology) Acquisition Program Integration/Acquisition System Management
PDR	Program Deviation Report
PEO	Program executive officer
SAE	Service acquisition executive
SAR	Selected Acquisition Report

Chapter One

INTRODUCTION

BACKGROUND AND OBJECTIVES

All major weapon system programs establish a program baseline early in the acquisition cycle which delineates cost, schedule, and performance targets for the program. The baseline is revised at subsequent milestones as the system proceeds through development and as more accurate information becomes available. Associated with the baseline is a set of cost, schedule, and performance thresholds. If the thresholds are exceeded, a review and assessment procedure is initiated in an attempt to understand why the threshold was "breached" and how the program can be brought back on track. Deviations from program baselines can be caused by the uncertainty inherent in complex system development programs as well as by internal and external events affecting the program throughout its acquisition cycle. Most programs experience events that require changes to their baselines at some point in their life-cycles.

The acquisition program baseline (APB) formalizes an agreement between the program manager and OSD acquisition decisionmakers by establishing and making explicit the desired program outcomes and performance expectations. This baselining process can be a useful management tool for acquisition managers by providing metrics for measuring program status and a process to respond to deviations from the plan.

Until recently, the baselining process applied a uniform formula to establish thresholds,[1] regardless of the fact that some deviations from the baselines are inherently more important than others. The result was that a large number of breached programs took significant time to rebaseline and could thus require the attention of senior acquisition managers over an extended period.

Recent changes in acquisition legislation, regulations, and directives allow for increased tailoring of the parameters included in the baseline and the thresholds associated with those parameters.[2] However, no criteria for appropriate tailoring have been established. An awareness of the relationship between program life-cycles and developmental events and the factors affecting deviations from the baseline can help acquisition decisionmakers develop appropriately tailored baselines and thresholds.

The overall goal of the research reported here is to enhance the usefulness of the acquisition program baselining process as a management tool for acquisition decisionmakers. Specific objectives include (1) to develop an analytic tool that can be used to analyze historical trends in the number, duration, and factors affecting APB breaches and (2) to analyze the relationship between program acquisition life-cycles and the factors affecting deviations from program baselines. The analytic tool (described in the Appendix) is meant to be used by the sponsoring office for monitoring the APB process.

A wide range of acquisition management related issues are addressed in this research. One issue concerns how a baseline is established. Baselines for major defense acquisition programs are developed by the program manager, approved by the service acquisition executive (SAE) or defense acquisition executive (DAE), and revised as appropriate at subsequent milestones. The key issue here involves understanding what information is available at different points in time and how it is used to reflect program risk in the baseline.

---

[1]Cost thresholds were determined as a 15 percent increase in R&D costs or a 5 percent increase in procurement costs. Schedule thresholds were based on a six-month slip from critical program milestones and events. See Chapter Two for a complete description.

[2]Federal Acquisition Streamlining Act of 1994, DoD Instruction 5000.1, DoD Regulation 5000.2-R; USD(A&T) Memo dated 27 September 1995.

Thresholds should reflect this program risk and the decisionmaker's level of acceptable risk.

Another important concern is identifying and characterizing the factors that affect changes from the baseline, resulting in threshold breaches. Some of these factors may be internal to DoD and thus subject to influence by changes in policy and procedure; some factors are exogenous or systemic and not controllable by DoD. Distinguishing between these two types of factors would allow acquisition officials to focus on events they can influence.

Perhaps the central challenge of the new APB process concerns how to establish appropriate thresholds. This involves understanding the factors affecting a decisionmaker's sensitivity to threshold breaches, including the level of acceptable risk as well as the magnitude of the breach and the difficulty and time required to fix the problem. A critical aspect concerns the rationale for the baselining process: What information is the process intended to provide affecting what types of decisions?

RESEARCH AND APPROACH

This research begins to address two broad policy issues. The first concerns how to discriminate among the different types of baseline breaches. Breaches are not inherently equal in importance or in their relative effect on the program, which suggests that management attention should be applied with discrimination. This implies the need for a set of criteria that can be consistently applied across programs to establish appropriate risk-based thresholds, given the preferences of decisionmakers. A consistently applied set of criteria will result in a tailored baseline process: differences among programs would be a function of risk preferences and attitudes of decisionmakers and unique program characteristics.

The second issue concerns how the APB document and process can be used to improve acquisition management, within the context of the current initiatives on acquisition reform. Various aspects of the APB process suggest that it can be a more effective management tool than as currently implemented.

As a first step in addressing these policy issues, we examine several specific research questions:

- How has the APB process worked in the past? This includes describing the process, why it was established, and how it currently works, as well as recording actual experience (frequency and type of breaches).
- What factors affect APB breaches? This involves a determination of the root cause of a breach, if possible, or at least construction of some part of the chain of events leading to the breach.
- To what extent are APB breaches associated with a program's acquisition life-cycle? The interest here is in understanding whether breaches are associated with program events in some way.

The research documented in this report was performed in two phases. Phase 1 included three tasks:

- *Determine the rationale for the baselining process in the current environment.* What information is it intended to provide and to whom? What decisions is this information intended to inform? Answers to these questions provide context for the analysis and should also be reflected in the guidelines or criteria that express decisionmaker sensitivity to different threshold breaches.
- *Characterize the problem.* This task developed a historical database that documented frequency of past threshold breaches as well as other aspects of the baseline process, such as the time needed to resolve breaches, events in process, and factors affecting threshold breaches.
- *Develop an analytic tool* that tracks and monitors the baselining process for each program, using the information in the historical database.

Several sources of historical information were used to develop the database and provide the substance of the analytic tool. The APBs themselves provided information on how many baselines a program had over the period of interest, and what changed from one baseline to the next. The Defense Acquisition Executive Summary (DAES)

monthly status summaries, prepared by the Office of the Under Secretary of Defense (Acquisition & Technology) Acquisition Program Integration/Acquisition System Management (OUSD(A&T) API/ASM), provided information on the number and duration of APB breaches. Program deviation reports (PDRs), submitted by program managers when a deviation from the baseline is formally acknowledged, provided information on factors affecting APB breaches.[3]

Our research approach also included extensive discussions with the Office of the Secretary of Defense (OSD) and service acquisition officials who are involved in or make use of the baselining process. These discussions helped resolve some apparent data conflicts and inconsistencies, as well as improve the interpretation of the data and analytical results.

Phase 1 of the research raised the question of when deviations to baselines occur in a program's acquisition cycle. Phase 2 expanded the analysis to examine the relationship between program acquisition life-cycles and the factors affecting deviations from program baselines. We constructed two schedule-related variables. The first measures program maturity (e.g., years past Milestone 2). This variable has proved to be a powerful explanatory variable in previous work at RAND on cost growth and schedule slip.[4] The second variable documents the specific activity going on when the deviation was revealed (e.g., test failures or successes, programmatic reviews, technical reviews, etc.). Both variables, derived from data in the Selected Acquisition Reports (SARs), provided a basis for analyzing patterns in the timing of changes to baselines. Data collected in Phase 1 on the factors affecting these changes were correlated with the life-cycle variables to determine whether patterns exist among programs at similar stages in the acquisition cycle. The idea was to enable acquisition decisionmakers to anticipate future breaches based on program life-cycle characteristics.

---

[3]These information sources have certain caveats associated with their use. These are described in Chapters Three and Four and the Appendix.

[4]See J. A. Drezner et al., *An Analysis of Weapon System Cost Growth*, RAND, MR-291-AF, 1993; and J. M. Jarvaise, J. A. Drezner, and D. Norton, *The Defense System Cost Performance Database*, RAND, MR-625-OSD, 1996.

ORGANIZATION OF REPORT

This report documents both Phase 1 and Phase 2 of RAND's research on the APB process. Chapter Two describes the previous APB process as well as the changes instituted in recent regulations—changes that can have a significant effect on the usefulness of the APB process as a management tool. Chapter Three presents macro-level trends in the number, type, and duration of APB breaches. Several metrics are presented and explanations for the observed trends are developed. Chapter Four begins to examine the factors affecting program breaches. The relationship between acquisition program life-cycles and APB breaches is examined in Chapter Five, exploring the hypothesis that certain types of breaches occur at certain points in the acquisition life-cycle.[5] Chapter Six summarizes the results of our analysis and presents observations about the APB process and what the process implies for acquisition management and oversight. Recommendations to enhance the usefulness of the APB process are also made.

An important part of the research was the development of an analytic tool for use by acquisition officials involved in the APB process. The Appendix briefly describes the structure of the tool and its underlying assumptions.

[5]All of the analyses presented in Chapters Three through Five can be broken down by military service. We performed this analysis, but few significant differences emerged during its course.

Chapter Two

ACQUISITION PROGRAM BASELINE PROCESS

GENERAL BACKGROUND

Acquisition program baselines (APBs) represent an agreement between the program manager, the program executive officer (PEO), and the milestone decision authority (MDA)[1] regarding critical program cost, schedule, and performance parameters. APBs are intended to enhance program stability and provide a reference point for measuring and reporting program status.[2] According to the Defense Acquisition Deskbook (September 1996):

> APBs serve as a means of obtaining corporate commitment for a program from the entire acquisition chain of command, measuring program performance, and establishing a "trade-space" for the program management team.

As a management tool, APBs are rough indicators of program stability. An approved APB indicates a program with no major programmatic, substantive, or administrative issues outstanding. A program in breach status indicates that one or more issues remain to be resolved.

---

[1]The MDA is the component acquisition executive (CAE) (usually the Assistant Secretary for Acquisition in the military service) for ACAT 1C programs and the defense acquisition executive (the USD(A&T)) for ACAT 1D programs.

[2]DoD Directive 5000.2, Part 11, 23 February 1991. Although this Directive has been superseded by DoD Regulation 5000.2-R (16 March 1996), the purpose of APBs remains consistent and relevant.

APBs are required of all major defense acquisition programs (MDAPs) in the demonstration/validation, engineering and manufacturing development (EMD) and production phases of acquisition.[3]

Cost parameters are generally the same for all programs and include development cost, procurement cost, military construction costs, and program average unit cost. Quantities are reported in APBs but not as a breachable parameter. Schedule and performance parameters are tailored to the specific program and may include key decision points in the schedule, and technical, operational, and support related performance indicators.

A parameter has a *target value* and a *threshold.* The target is a management goal (objective); the associated threshold is a level above (or below) the target that when breached triggers a senior management review. The difference between the target and the threshold reflects a condition that brings into question the value of the program. Targets and thresholds are meant to be reasonable and realistic. Thresholds are derived from the targets and minimum acceptable operational requirements specified in the Operational Requirements Document required of each MDAP.

APBs are revised at major milestone decision points in the acquisition process. Three types of APBs are associated with major milestones and acquisition phases: *concept* (Milestone 1 and the demonstration/validation phase), *development* (Milestone 2 and the EMD phase), and *production* (Milestone 3 and the production phase). The specific parameters listed, and their associated objective and threshold values, may change for each type of baseline. In fact, such changes are expected as the information available to estimate program performance improves over time as the program matures. Concept baselines use broad performance metrics, while development baselines are at a more detailed system specification level. Production baselines essentially update development parameters.

---

[3]Originally, APBs were required only beginning at EMD. This requirement was eventually extended to all programs beginning at Milestone 1 (approval for demonstration/validation). Acquisition Program Baseline Point Paper, Transition Book, 1992 (OSD).

The Defense Acquisition Executive Summary (DAES), established in 1988, is both an internal report and a review process. The report is standardized across programs and covers the same programs as the SAR (acquisition category [ACAT] 1C and 1Ds).[4] Programs are divided into three groups (A, B, and C); each group reports quarterly on a staggered schedule. Thus, each program submits a new DAES every three months to provide information as early as possible on program execution, policy decisions, and problems affecting the program.[5]

The DAES and SAR track program performance quarterly against the parameters specified in the APB document. Breaches—deviations above the threshold for a given APB parameter—are tracked monthly by OUSD(A&T)API/ASM and reported at DAES monthly status meetings. These meetings, chaired by the Deputy USD(A&T), include the component acquisition executives (CAEs) and other senior OSD acquisition, program evaluation, and financial management officials.

SOME HISTORY AND A DESCRIPTION OF THE INITIAL PROCESS

DoD Directive 5000.45 (August 1986) mandated DoD-wide baselining of major systems and specified formats, responsibilities, and approval authority. This action represented the implementation of a 1986 Packard Commission recommendation to use baselining as a way to improve program stability. Apparently, implementation did not occur until the DAE established baselines in February 1988, although several formal APB documents are dated September 1987. As of October 1988, there were 75 approved APBs (17 Army, 35 Navy, 23 Air Force), 9 in progress, and 10 yet to be submitted.[6] While APBs

[4]ACAT 1 programs are defined according to the same criteria that define an MDAP, that is, more than $355 million (FY96 dollars) in RTD&E expenditures, or more than $2.135 billion in eventual procurement expenditures. For ACAT 1C programs, the milestone decision authority is the service acquisition executive; for ACAT 1D programs the MDA is the defense acquisition executive.

[5]Larry Gwozdz, "Overview of the Defense Acquisition Executive Summary (DAES) Reporting Process," briefing.

[6]Major Program Baselining Point Paper, API/ASM Transition Team Background Book, 28 October 1988 (prepared by J. Ferrara).

have been submitted, approved, and breached since 1988, status tracking has been systematic only since 1992.

APB policy was initially established by DoD Directive 5000.2-M, Part 14 (February 1991). APBs are prepared by the program office and submitted up through the service acquisition chain of command to the CAE, who is the approval authority for ACAT 1C programs. APBs for ACAT 1D programs are forwarded to the DAE for approval, through the Deputy Director, Acquisition Systems Management, OUSD(A&T)API. APB documents are "coordinated" with relevant functional offices both within the services and OSD. These offices represent developmental testing, operational testing, and financial management. A designated official in each service is responsible for tracking and coordinating the APBs. OUSD(A&T)API/ASM is responsible for tracking all APBs, as well as reviewing DAES submissions each month to identify breaches. These breaches are then reported each month at the DAES monthly status meetings.

As initially established, the difference between the threshold and the target was the same for all programs regardless of the unique programmatic or technical characteristics of the program:

- Cost: 15 percent increase in research, development, test, and evaluation, 5 percent increase in procurement, 15 percent increase in military construction, or a 15 percent increase in procurement average unit cost.
- Schedule: six-month slip in a specified parameter.
- Performance: depended on the specific parameter; for many it was any change from the stated goal.[7]

When a program manager believed that a threshold would be exceeded, a Program Deviation Report (PDR) had to be submitted. A baseline change request (BCR) could be submitted concurrently, or at a later date after the baseline had been reestimated to incorporate the resolution to whatever issue caused the breach. The CAE had 45 days from receipt of the PDR to form a team to review the breach and

[7]DoD Directive 5000.2-M, Part 19, February 1991.

the reasons for the breach, and to recommend a course of action to the DAE.

Thresholds are intended to represent the minimum acceptable requirement for a parameter. Thresholds establish "deviation limits" and define the cost, schedule, and performance trade-off space available to a program manager without a requirement for prior approval from the Milestone Decision Authority (MDA). Key parameters to include in the APB are "those that if the thresholds are not met, the milestone decision authority would require a reevaluation of alternative concepts or design approaches."[8]

As part of routine program management activities, the program manager maintains a "current estimate" reflecting the current cost, schedule, and performance trade-offs and expected outcomes at program completion. Breaches, or deviations, occur when the current estimate exceeds the threshold value for a parameter in the APB. Since both the DAES and SAR contain the same parameters as the APB, breaches can be identified by comparing the current estimate to the approved program.

RECENT CHANGES

The Federal Acquisition Streamlining Act of 1994[9] (FASTA) was the first of several legislative and policy initiatives that changed elements of the APB process. FASTA (1) allows increased tailoring of the content of APBs by no longer specifying content or deviation thresholds; (2) gives the Secretary of Defense discretion to set guidelines for this tailoring, and for reporting, reviewing, and resolving APB breaches; and (3) states that no funds may be obligated for programs in EMD or production without an approved baseline. The tailoring provision potentially allows the APB to become a more useful and realistic management tool. The restriction on obligations sets up a strong incentive to resolve APB breaches.

A related FASTA provision requires that the Secretary of Defense assess whether "major and nonmajor acquisition programs of the

[8]DoD Directive 5000.2, Part 11, 23 February 1991.

[9]Conference Report, Federal Acquisition Streamlining Act of 1994, August 21, 1994.

Department of Defense are achieving, on average, 90% of cost, performance, and schedule goals. . . ." If this criterion is not met, a program review is required to determine whether there is a continuing need for the problem program. Although the legislation does not state it explicitly, one interpretation is that no more than 10 percent of all parameters in all APBs can be breached at any time. This requires OSD to count APB parameters and breaches individually. Since a single breach often involves several parameters, the potential level of effort required is significant; some programs (e.g., the F-16) have more than 100 cost, schedule, and performance parameters listed in the APB.

A policy memo from USD(A&T) which implemented the APB related provisions of FASTA[10] was repeated in DoD Regulation 5000.2-R (15 March 1996). Highlights of the new APB process and policy statement, and changes to the former process are briefly described here:[11]

- Programs must still specify cost, schedule, and performance objectives and thresholds. If threshold values are not specified, the threshold value for performance parameters is the same as the objective, the threshold value for schedule is the objective plus six months (as before), and the threshold value for cost is the objective plus 10 percent (vice 15 percent for RDT&E/5 percent for procurement) (Section 3.2.1).[12]
- Program managers are explicitly allowed to make tradeoffs among cost, schedule, and performance within the trade space defined by the objective and threshold values without MDA approval. The exception is that key performance parameters validated by the Joint Requirements Oversight Council (JROC) may not be changed without JROC approval (Section 3.2.1).
- APBs are required at program initiation, not just at EMD. In some cases, this might include pre-Milestone 1 programs if they are well enough defined. Performance parameters must explic-

[10]Memorandum from Under Secretary of Defense (Acquisition and Technology), 27 September 1995.

[11]DoD Regulation 5000.2-R, 15 March 1996.

[12]Note that changes in thresholds will change the definition of "breach." Thus, we are likely to see a significant deviation from historical trends in breach frequency.

itly include supportability and environmental requirements (Section 3.2.2).

- The APB content (parameters included) should be tailored as appropriate. The parameters should be limited to the most important—those that if the thresholds are not met would require a reevaluation of alternative concepts or designs. The values of the parameters should define the program as it is expected to be deployed. Performance parameters at Milestone 1 may be broadly stated, but should become more specific as the program matures. The performance parameters should include the minimum required to define operational effectiveness, schedule, technical progress, and cost (Section 3.2.2.2). (Total quantity appears to have become a "breachable" cost parameter.)
- No funds can be obligated for an MDAP after the program enters EMD or later phases without an approved APB, unless a waiver has been obtained from USD(A&T).
- A program deviation—baseline breach—occurs when the program manager has reason to believe that the current estimate for a parameter is not within its threshold value. The program manager is required to notify the MDA immediately and to provide reasons for the deviation and the action required to resolve the issue within 30 days. Programs are expected to be back within an approved APB within 90 days or the program manager should estimate an alternative date (Section 6.2.1.1).

An additional recent consideration is that the APB process will become a more integral element of acquisition management through the implementation of "stretch goals."[13] A recent internal review of acquisition management and oversight processes recommended "using a continuous improvement process,[to] increase the number of MDAPs that are within their approved baseline at a given time from the current 80–85 percent to 95 percent within 3 years."[14] Officials recognize that since some APB changes are external to DoD

[13]Stretch goals are significant but achievable management challenges, often requiring a fundamental change in the way business is conducted.

[14]*Stretch Goals and Metrics for the Reengineered Oversight and Review Process*, Final Recommendations as of October 25, 1995, briefing.

acquisition management processes (e.g., Congressional budget cuts), achieving 100 percent conformance is not feasible. Based on historical analysis (see Chapter Three), maintaining 95 percent of MDAPs within their approved baselines will be a difficult goal to achieve. To achieve the 95 percent goal, additional attention needs to be paid to tailoring APB contents (parameters), goals, and thresholds, as well as the factors affecting breaches and the duration of those breaches.

Chapter Three

TRENDS IN BREACHES OF ACQUISITION PROGRAM BASELINING

The Office of the Secretary of Defense (OSD) has used acquisition program baselines to monitor the progress of major weapon system programs since 1988. As described in Chapter Two, a flag is raised whenever a cost, schedule, or performance threshold is breached. Virtually every major defense acquisition program with an approved baseline has experienced a baseline breach at one point or another. This chapter looks at trends in the number of baseline breaches that have occurred over time, and the duration of the breaches. As we will see in later chapters, not all breaches are alike, and there are various reasons for a program to breach its baseline. This chapter merely accounts for the number of breaches that have occurred.

DATA SOURCES

Data for these analyses are from the monthly Defense Acquisition Executive Summary (DAES) Monthly Status Reports and the APB for each major weapon system. The DAES reports indicate whether a program baseline was breached in a given month and the type of parameter that was breached (cost, schedule, or performance). The month in which a breach is reported is assumed to be the date the program breached its thresholds; the month an approved APB is issued is assumed to be the date the breach was resolved. These data are used to show trends in the number of programs in breach status each month and the duration of the breach. Data from the DAES are available beginning in April 1992; therefore, the trends shown in the analysis are for the April 1992–June 1996 period.

The APBs provide information on the number of baselines issued for each program, the type of parameters that were changed by each new baseline (cost, schedule, or performance), and what type of changes were made to the baseline. These changes fall into four categories:

1. Parameter thresholds were breached.
2. Baseline estimates were changed even though parameter thresholds were not breached.
3. New threshold parameters were added or existing parameters were deleted.
4. New estimates were an improvement to the previous baseline targets.

Approximately 120 programs had approved baselines over the period covered by the analysis. Most of these programs had several baselines, so the analysis covers approximately 500 baselines. The data from these sources are in two Excel spreadsheets. These spreadsheets are integrated with the data on the factors affecting the breaches in an integrated program analysis tool that was provided to OSD. The spreadsheets are described in detail in the Appendix.

This analysis sought to identify broad trends over time in the data. It addressed two questions: Are the number of programs in breach status declining over time? and Is the average duration of these breaches declining over time?

NUMBER OF BREACHES

The DAES Monthly Status Reports show the number of programs in breach each month. On average, 28 programs, or 25 percent of all active MDAPs, were in breach each month over the 1992–1996 period. The number of programs in breach status has declined steadily since 1992 both in absolute terms and as a percentage of active MDAPs. As seen in Figure 3.1, the number of programs in breach status in any given month declined from a high of 48 in 1993 to a low of 8 in November 1995, with an increase to 20 to 23 during the first part of 1996. The overall trend is a reduction in the number of programs in breach status over time, but there are several spikes in the

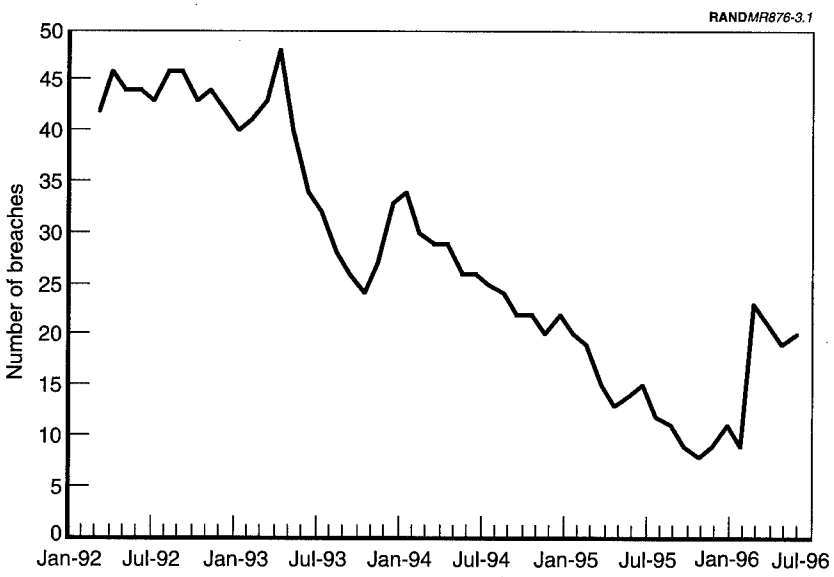


Figure 3.1—Number of Acquisition Program Baselines in Breach by Month, 1992–1996

number of breaches. These spikes may be associated with the budget cycle or other major acquisition program reviews. The programs comprising the spikes share little in common in terms of their characteristics, or the type of breach that occurred. In some cases, the spikes may represent a return to the underlying trend. For example, very few breaches were reported in the second half of 1995 through February 1996. The March 1996 spike may represent a correction of sorts, reflecting problems in programs that existed but were not reported earlier.

While the number of programs experiencing baseline breaches declined over this period, so did the number of active programs. The number of MDAPs declined from 113 in 1992–93 to 81 in 1995–96.[1] Figure 3.2 shows the number of breaches as a percentage of MDAPs

[1]MDAP list developed by OUSD(A&T)API/ASM. The list of MDAPs is issued in July of each year.

active in that year. The slopes and shapes of the lines in Figures 3.1 and 3.2 are similar, suggesting that the trend depicted is not explained by a decline in the number of active MDAPs. Approximately 45 percent of the MDAPs were in breach in early 1993, compared to 20 percent in July 1996. The low point was November 1995; only 7 percent of the active programs were in breach status.

This downward trend in the number of programs in breach each month can potentially be explained in several ways. First, the management of the APB process may have improved. The process was relatively new in 1992, and it took time for program managers and OSD to learn how to deal with program breaches. Second, management may have paid increased attention to the process. The number of breaches is reported each month at the DAES monthly status meeting. The large number of breaches in the early 1990s generated concern, and OSD has focused attention on reducing the number of programs in breach at any given time. Third, the decline may reflect problems with the data. Evidence shows that the number of ACAT

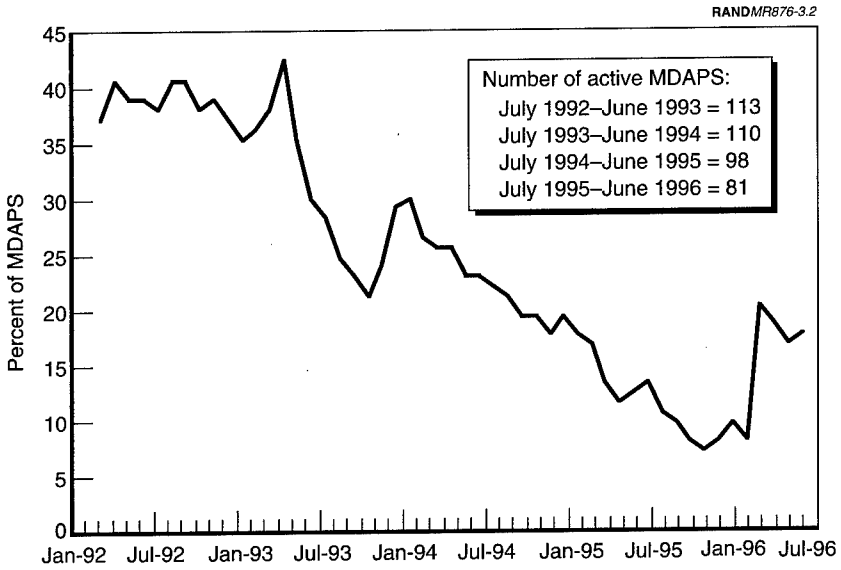


Figure 3.2—Number of Acquisition Program Baselines in Breach by Month, 1992–1996, As a Percentage of Major Defense Acquisition Programs

1C programs have not been consistently reported or counted in the data. Even ACAT 1D programs are not reported consistently. For example, no breaches were reported for the Air Force between September and December 1995, even though at least one Air Force program (the F-22) breached its baseline during that period. To the extent that breaches are less likely to be reported today than previously, the extent of the decline in the number of breaches would be overstated.

The number of breaches in a given month is equal to the number of breaches carried over from the previous month, plus any breaches that occurred in that month, less any breaches that were resolved since the previous month.

Figure 3.3 shows the source of the changes or turnover in the number of breaches. The figure shows the total number of breaches, the number of breaches carried over from one month to the next, the number of new breaches each month, and the number of breaches

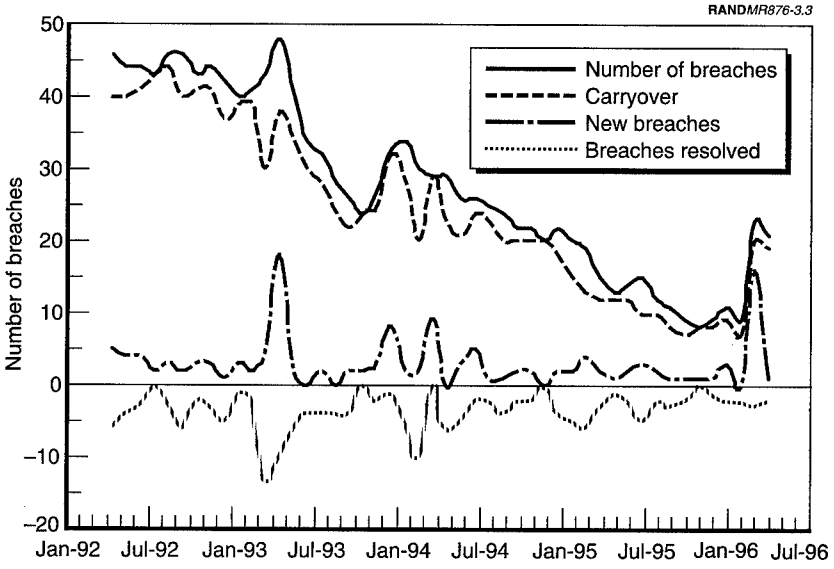


Figure 3.3—Components of Turnover in the Number of Breaches by Month, 1992–1996

resolved each month. Note that the number resolved is less than or equal to zero because it represents a reduction in the number of programs in breach status.

The number of new breaches each month and the number of breaches resolved each month are relatively stable. The spikes in the number of new breaches tended to increase the total number of programs in breach, though on occasion the increase was offset by an increase in the number of breaches resolved. In general, more breaches are resolved than are added each month, leading to the decline in the carry-over in the number of programs in breach from one month to the next and the total number of programs in breach each month.

Figure 3.4 repeats the data on the number of new breaches and the number of breaches resolved, as a percentage of major defense acquisition programs (MDAPs). The downward trend remains after adjusting for the reduction in the number of MDAPs, which implies that the number of breaches is declining faster than the number of MDAPs. Again, the downward trend depicted in the figure appears to be an actual trend, though the drivers of the trend are uncertain.

Figure 3.5 shows the number of breaches by the type of parameter breached. Throughout most of the period, the schedule parameters breached most often. Cost parameters breached almost as often; in fact, during much of 1993 and part of 1994, they breached more often than the schedule parameters. Performance parameters were breached least often throughout the entire period. Surprisingly, no performance breaches were reported between March 1995 and February 1996. The relatively low number of performance breaches supports the contention that program managers trade cost and schedule demands in order to meet performance goals. Figure 3.5 also shows that both cost and schedule breaches contributed to the several spikes in the number of breaches.

CHARACTERIZING CHANGES TO THE BASELINE

Almost every program experiences at least one change to its baseline at some point in its life. But not all changes are equal. In fact, not all changes involve breaches of baseline thresholds. In some cases, new

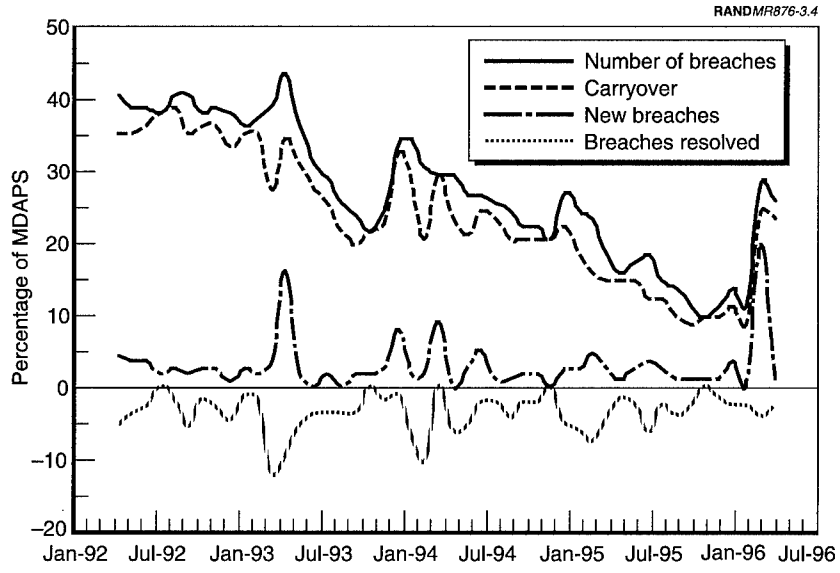


Figure 3.4—Components of Turnover in the Number of Breaches As Percentage of MDAPs, by Month, 1992–1996.

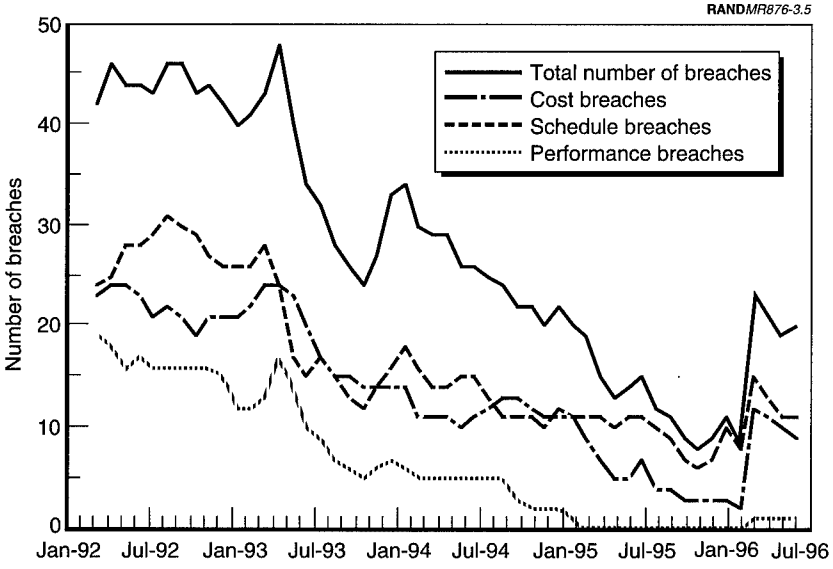


Figure 3.5—Number of Breaches by Type of Parameter Breached, by Month, 1992–1996.

baselines were issued to reflect changes to cost, schedule, or performance estimates that were within the thresholds of the previous baseline. In other cases, new parameters were added to the baseline, or old parameters deleted. On relatively rare occasions, the baseline changes reflect more optimistic estimates—the program would cost less, would meet its schedule milestones earlier, or would perform better than the previous baseline estimate. Table 3.1 summarizes the type of changes to program baselines for all major programs.

The table shows the number of baselines with each type of change. Because more than one type of change may be made to each baseline, Table 3.1 puts the type of change into a hierarchy:

- If a parameter threshold was breached, the type of change is coded as a breach, regardless of what other changes were made.
- If a parameter target is revised, but no thresholds were breached, the type of change is coded as a revision.
- If a parameter is added or deleted, but no thresholds were breached or targets revised, the type of change is coded as an addition or deletion.
- If a parameter target is improved, and there were no breaches, revisions, or additions/deletions, the type of change is coded as an improvement.

Table 3.1

Number and Type of Changes Made to Program Baselines (through June 1996)

Type of Change	Cost Parameters	Schedule Parameters	Performance Parameters	All Parameters
Parameter breach	141	130	27	228
Revision to parameter estimates	58	36	43	47
Addition or deletion of parameters	5	36	25	13
Improvements to baseline targets	15	5	9	6
Total	219	207	104	294

SOURCE: Acquisition program baselines.

This coding was done for the cost, schedule, and performance sections of each baseline separately, and for the baseline as a whole.

Table 3.1 shows that most changes to baselines are breaches. Of the 294 baselines changed during the period examined by this study, 228 involved breaches of parameter thresholds. Almost two-thirds of the changes to the cost and schedule parameters of baselines involved at least a breach of a threshold, while the performance parameters were revised more often than they were breached. This table also shows that the cost and schedule sections of the baselines were changed almost twice as often as the performance section.

Of the 120 programs covered in our database, only 19 programs issued a single baseline (had no breaches). These were either very young or very mature programs. Many of the young programs were terminated within a year or two of the initial baseline; many of the older programs may have breached prior to 1988, a period not covered by our data.

DURATION OF PROGRAM BASELINE BREACHES

How long does it take OSD and the program offices to resolve baseline breaches? Are breaches being resolved more quickly now than in the past? Or are more programs or fewer programs in breach for extended periods of time? To address these questions, we developed several measures of the duration of program breaches.

We first look at the distribution of the total length of time (cumulative months) programs spend in breach status. Figure 3.6 shows the distribution of the cumulative total number of months of the breaches for the programs that were in breach through June 1996.[2] A significant number of these programs have spent a substantial amount of time in breach. The V-22, for example, was in breach for 49 consecutive months over this period. A program could be in

[2]While breach data have only been formally tracked since April 1992, many programs had been in breach for substantial periods before that (e.g., the RAH-66 Commanche had been in breach 21 months as of April 1992). While we capture these programs here, if a program had a breach which began and was resolved prior to April 1992, it is not in the database. If these data were available, we would expect the distribution shown in Figures 3.6 to change somewhat.

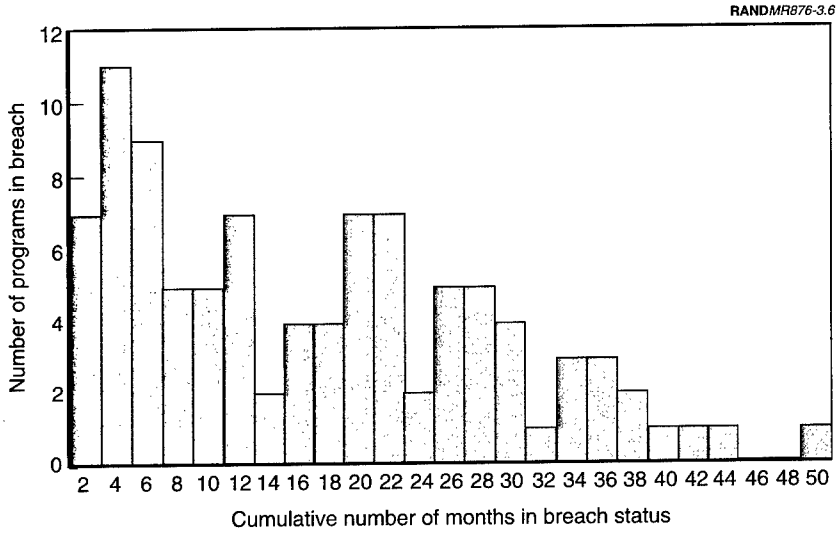


Figure 3.6—Cumulative Time in Breach Status

breach continuously if it is in flux, which would delay the resolution of the problem. On the other hand, while the initial breach may have been resolved relatively quickly, the program may have breached several times over the period. For example, the F-22 has had 5 baselines issued since February 1992; T-AGOS had 7 baselines since May 1992. This may indicate that the underlying cause of the breach was not addressed in the new baselines.

Figure 3.7 shows the distribution of the cumulative number of months programs were in breach during 1992, 1993, 1994, and 1995. The distribution tends to shift to the left in the later years. While a considerable number of programs were in breach for 10 months or more of 1992, only 2 were in breach that long in 1995—an indication that the average duration of program breaches has in fact declined over time.

Figure 3.8 shows essentially the same data as Figure 3.6, except the unit of analysis is an individual baseline, rather than a program. These data should be interpreted as the time it takes to resolve a

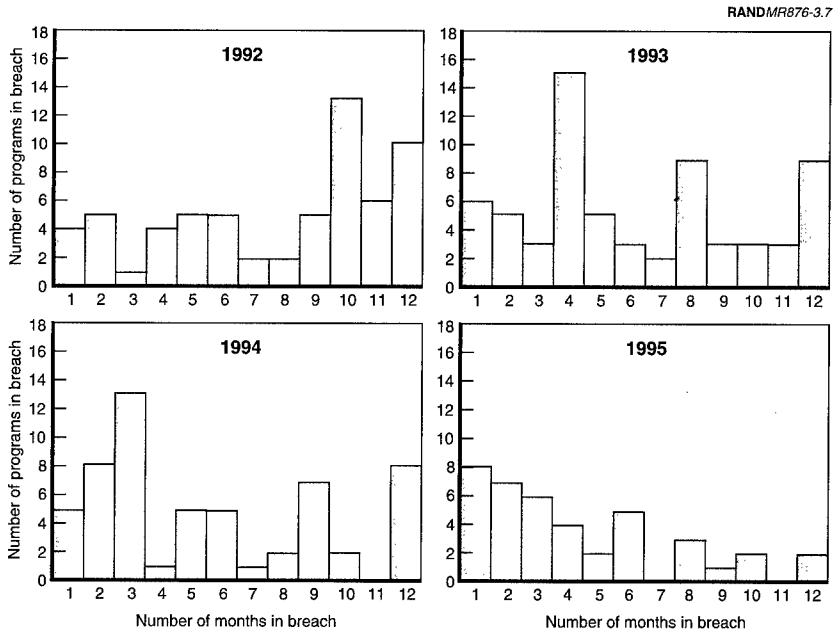


Figure 3.7—Distribution of Number of Months in Breach, by Year

given baseline breach. Most breaches are resolved within 12 months of their breach date: 56 percent are resolved within 6 months. However, a significant number of breaches require over a year to resolve, with some requiring over two years.

Another measure of duration is the average length of time programs were in breach at the time the breaches were resolved.[3] For example, new baselines were issued for 8 of the 47 programs in breach in the first quarter of 1993. The average duration these 8 programs were in breach was 4 months. This calculation was carried out for each quarter, from the second quarter of 1992 through the first quarter of 1996; the results are shown in Figure 3.9. The height of each bar rep-

[3]A program is in breach if one or more of its baseline parameter thresholds has been exceeded. A breach is resolved when all parameter estimates are brought back within their respective thresholds.

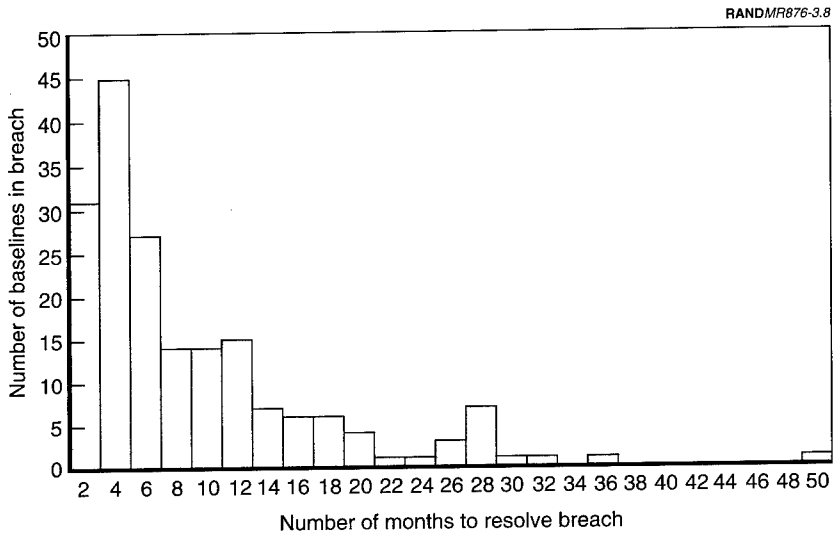


Figure 3.8—Distribution of Number of Months in Breach

resents the average duration of the breaches for the programs removed from breach status in that quarter. The number on the left at the top of each bar is the number of breaches resolved that quarter. The number on the right is the total number of programs in breach in that quarter. For example, in the second quarter of 1992, 51 programs were in breach, 11 of which were resolved that quarter, and these 11 programs had spent an average of 5 months in breach at the time their breaches were resolved.

The average duration of the breaches fluctuates over time, with no distinguishable pattern. If program breaches that have persisted for several months or years are resolved and fewer programs are in breach for lengthy periods of time, we would expect a downward trend in the average duration of breaches. While the backlog of breaches was being reduced over this period, the average duration of

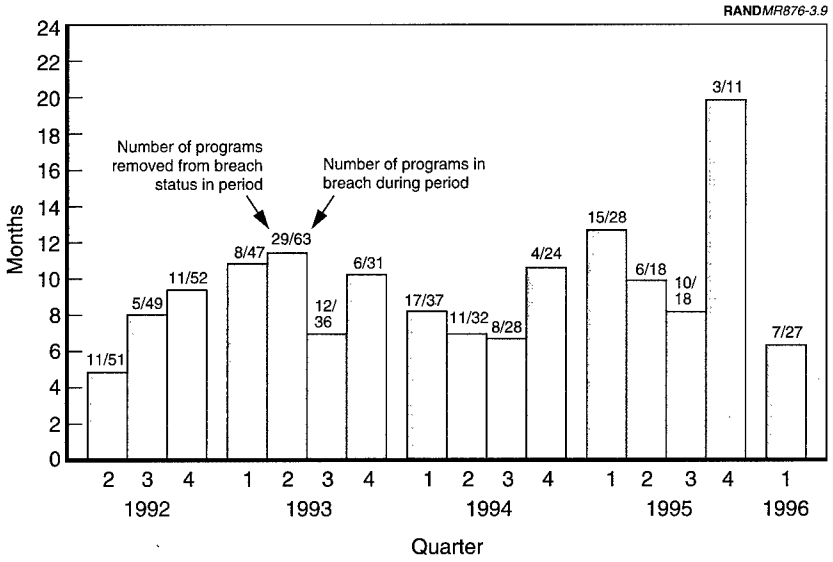


Figure 3.9—Average Duration of Breach When Program Removed from Breach Status

the breaches did not change.[4] In fact, this measure is somewhat problematic. A single breach may greatly influence the height of one of the bars. For example, the average duration of the breaches resolved in the last quarter of 1995 is close to 20 months because the 32-month breach of Maneuver Control System (Army Tactical Command & Control System) (MCS [ATTCS]) was resolved in December 1995. This is not an indication that OSD and the program offices were resolving breaches more slowly at the end of 1995; on the contrary, they were able to resolve a long-standing problem.

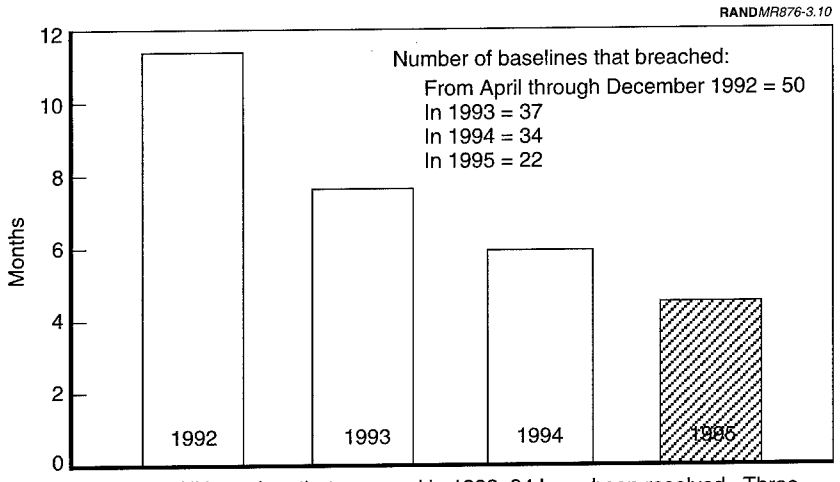
As a final measure, we calculated the average duration of program breaches by the year in which the breach began. For example, 46 programs breached during 1992; these programs were in breach an average of just over 12 months. Figure 3.10 shows clearly that breaches that occur later are being resolved more quickly. The aver-

[4]We also calculated error intervals around the mean (height of bar in Fig. 3.8) based on one standard deviation in order to detect underlying trends. No trend was detectable.

age has dropped from just under a year to less than 6 months. (Note: if the three breaches yet to be resolved from 1995 are resolved at the end of 1996, the average duration of the 1995 breaches will be approximately 6 months.)

SUMMARY

Between April 1992 and June 1996, an average of 28 programs were in breach status each month. The overall trend in the number of breaches is downward, driven by a decline in the number of breaches carried over from one month to the next. Since January 1995, the average number of programs in breach each month was 14. An average of 25 percent of active major defense acquisition programs were in breach status each month during the same period. The decline in the number of breaches persists even if we take into account the approximately 30 percent decline in the number of active major de-



NOTE: All breaches that occurred in 1992–94 have been resolved. Three baselines that breached in 1995 remain in breach as of May 1996.

Figure 3.10—Average Duration of Breaches by Year in which Breach Began

fense acquisition programs. Since January 1995, on average, 12.5 percent of active MDAPs were in breach compared to close to 40 percent during 1992.

Most programs breach their baselines at least once during their life-cycles. Some programs have had as many as nine baselines over their life-cycles. Most of the changes to program baselines are to the cost and schedule portion of the baselines. The majority of the changes are due to breaches of baseline thresholds, though a sizable share of the changes were revisions that did not breach the threshold. The performance section of the baseline was changed less often; the majority of these changes were revisions to the performance targets, not breaches of the thresholds.

The average length of time a program spent in breach over the period was just over 9 months. The average length of time tended to decline for breaches that began in more recent periods, independent of any effect of program maturity (see Chapter Five). A significant number of programs were in breach for over 20 months. Consistent with the decline in the average duration of the breaches, fewer programs are in breach for extended periods today than earlier in the period.

Chapter Four

FACTORS AFFECTING APB BREACHES

Deviations from program baselines occur for a variety of reasons. The root cause of APB breaches may be a simple event related to the difficulty of applying technology in a particular case or a similar factor related to the technical, political, and economic uncertainty inherent in weapon system development and production programs. The causal pathways can be very complex: a technical problem may result in a test failure which causes a program restructuring, but due to the availability of test resources cannot be accommodated within the six-month milestone threshold. The resulting schedule breach may then cause Congress to reduce outyear budgets, resulting in additional schedule and cost breaches.

Several parameters may breach at the same time for the same reason. Alternatively, several breaches may occur simultaneously but for independent reasons. Or a single parameter may breach for several independent reasons, each one of which could have resulted in a breach. Additionally, multiple cost, schedule, or performance parameters can breach at the same time. Sorting out the root cause and causal pathways is a challenging investigative task.

This chapter attempts to improve our understanding of the factors affecting deviations from program baselines. Our research goal is to determine the causes of baseline breaches. One important policy relevant goal is to be able to distinguish between factors that are potentially controllable by officials within DoD and factors that are external to DoD's acquisition management processes. This information would allow DoD to tailor its response, focusing significant attention on breaches whose prevention or resolution it can influence.

TAXONOMY AND DEFINITIONS

In conjunction with OUSD(A&T), we developed a taxonomy of factors affecting APB breaches and a set of categorization rules appropriate to both our purpose and available data.

We adopted a modified hierarchical taxonomy to account for the limitation of the source data in identifying root causes and the potential for multiple factors to affect a single or several independent breaches.

- The taxonomy is divided into two levels. The first level consists of broad issue-oriented categories. The second level is at a more detailed level and reflects actual events and decisions.
- Categories are mutually exclusive at both first and second levels.
- Coding is done for each baseline/breach for each program at the second-order level. Data are then aggregated up to first-order categories. Multiple second-order factors within a single first-order category are counted only once at the higher level.
- A single dominant factor will be identified if possible. However, in some cases there can be more than one independent factor affecting a particular breach, and/or multiple independent factors affecting multiple breaches.
- Use of the "other" categories is minimized.

Definitions are provided in the following format:

- FIRST ORDER FACTOR: definition/description
  - •• *second order factor*: definition/description

The taxonomy of factors affecting deviations from program baselines has six first-order factors and 22 second-order factors, including the "other" category:

- FUNDING RELATED: changes to funding/budget profile, often affecting quantity, sometimes related to cost.
  - •• *congressional reduction*: reduction of previously expected/budgeted amount by congressional action in appropriations/authorization actions.

- *DoD reduction*: reductions due to OSD or Service actions associated with the POM or PPBS cycle.
- *shortfall*: not enough funds in original plan (underestimation).
- *reprogramming*: addition of previously unbudgeted amount, or reallocation among accounts or programs.
- *other*: other budget related actions not classified into above categories either due to poor information or different class of action.

- TECHNICAL RELATED: technology or engineering design related problems, often identified during testing. Includes hardware and software.
  - *technical difficulty*: identified deficiency or technical problem.
  - *feasibility*: pushing the state-of-the-art too hard, too challenging, physically impossible (perhaps a reflection of an unrealistic estimate).
  - *other*: other technology based problems.
- CONTRACTOR RELATED ISSUES: performance, management or business base related.
  - *late deliveries*: product, system, component delivered late. Includes government furnished equipment (GFE).
  - *quality control*: production process related.
  - *labor problems/strikes*: includes poor management, inexperience.
  - *business base*: increase in overhead at plant/firm due to termination of other unrelated programs.
  - *other*: other contractor-based issues.
- REQUIREMENTS CHANGES: changes to the technical characteristics of the system or force structure, usually directed from above the program office.
  - *quantity change*: non-funding related quantity changes, often due to force structure changes or changes in priority.

  - *change in specification, mission, capability*: specific aspects of performance changed as a result of user evaluation or assessment.
  - *other*: other requirements based issues.
- PROGRAM RESTRUCTURING: change in acquisition strategy that captures revised guidance as source of change. Not directly associated with funding related issues or specific weapon system requirements.
  - *strategy change*: changes in process, approach, procedures, phasing, competition, contracting, etc.
  - *revised guidance*: direction from outside program office to revise approach. Directed change.
  - *test resource availability*: test facilities or unit becomes unavailable due to changes in priority or unit deployment.
  - *other*: other program restructuring related actions.
- OTHER: catch-all category, including particularly hard "gray area" breach explanations.
  - *misestimation*: reflects inherent uncertainty in estimating baselines not captured elsewhere, including improved information or methods.
  - *other*: fits into no existing category or information is too poor to classify.

CAVEATS

The caveats and limitations affecting this part of the analysis derive almost entirely from the source of the data. As noted in Chapter Two, the program manager is required to submit a Program Deviation Report (PDR) explaining the reasons for the APB breach. We obtained copies of the PDRs for as many breaches as possible. Because PDRs for every breach were not available, we do not have them for a large number of breaches in the database. Sometimes we were able to substitute summary statements made in cover letters written by the program executive officer (PEO) or SAE forwarding the PDR to OSD.

The PDRs themselves pose another limitation. PDRs span a range of detail from simply acknowledging the breach to several pages of detailed technical information on why a breach occurred and its implications for all aspects of the program. In general, most PDRs leaned toward the short summary format. The statements made in the PDRs are mostly general, suggesting that other factors we have no insight into may have influenced the breach.

Acquisition management is a complex process and the root cause of a breach can rarely be explained in a short sentence. Further, the program manager's dominant incentive is to provide as little detail as possible without specifying exact causes and causal pathways. In fact, the program office usually writes the PDRs in passive voice, implying that the breach in question merely "happened" rather than that it resulted from a set of events or decisions. This is a reflection of a larger problem regarding the incentives inherent in the process. Thus, our analysis cannot claim to have identified the root causes of APB breaches or the dominant (or common) causal pathways. Nevertheless, we believe that some insight is gained through a study of the PDRs.

RESULTS

Figure 4.1 shows the distribution of first-order factors for all baseline breaches for which we have data (PDRs). Note that there is no dominant factor at this level. Funding, program redirection, requirements, and contractor related factors all affect about 20 percent of the APB breaches. Technical related problems, usually found during either contractor or government test programs, affect breaches about 12 percent of the time, a surprisingly small frequency.

There are few significant differences among the services at the first-order factor level. The Navy appears almost identical to the DoD average. Program breaches in the Army are somewhat more often affected by funding related factors (30 percent). The APB breaches in the Air Force are somewhat less affected by requirement changes (13 percent).

Figure 4.2 shows the distribution of second-order factors affecting APB breaches across DoD. The largest factor is nonfunding related

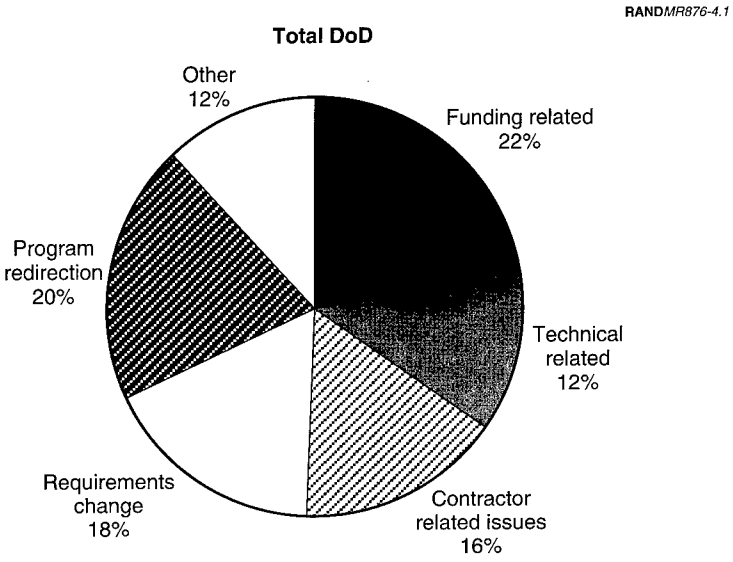


Figure 4.1—First-Order Factors Affecting APB Breaches

quantity changes. Revised guidance and technical difficulty are the next most common second-order factors, followed by misestimation and DoD reduction. These five categories account for about 46 percent of the total. In general, the results suggest that a significant number of APB breaches are affected by a wide range of factors. Note that at the second-order level, technical difficulty shows up as one of the most common factors, but given the wide range of second-order factors, it does not dominate at the first-order level.

Some differences appear among the services at the second-order factor level. The Air Force is dominated by revised guidance (10.6 percent), misestimation (11.4 percent), technical difficulty (9.8 percent), and DoD reduction (9.8 percent). The Navy is dominated by quantity changes (13.0 percent), technical difficulty (9.1 percent), and changes in specifications, mission, and capability (8.4 percent). The Army is also dominated by quantity changes (14.7 percent), followed by revised guidance (11.9 percent), DoD reductions (10.1 percent), and reprogramming (10.1 percent).

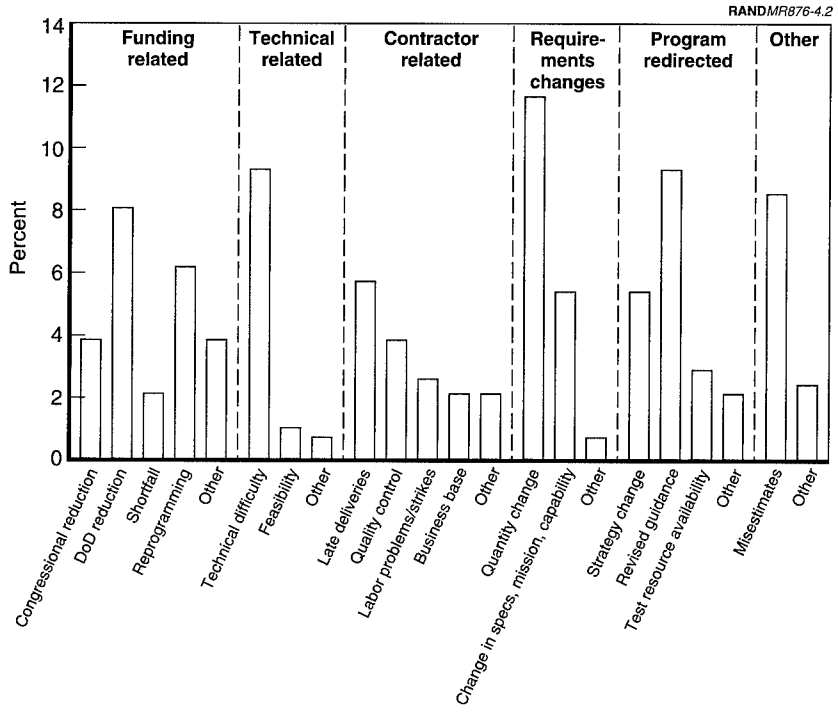


Figure 4.2—Second-Order Factors Affecting APB Breaches

SUMMARY

Identifying the factors affecting baseline breaches is challenging, given the available data. Unfortunately, data do not exist to support the identification and analysis of root causes. Nevertheless, some interesting observations can be made from the factors analysis presented in this chapter:

- Baseline breaches usually result from a complex chain of events and decisions. At the program level, these events and decisions are unique to each program.

- Multiple factors are common, both in terms of independently causing the same breach or independently causing independent breaches.
- There are no dominant factors at either level of our taxonomy. First-order factors are about evenly distributed. While some differences emerge at the second-order level, five factors (DoD reductions, technical difficulty, quantity changes, revised guidance, and misestimation) are about equally common.

Although we did not perform a detailed analysis of internal vs. external factors, a subsequent chapter illustrates how these results can usefully illustrate the distinction between those factors DoD can potentially influence and those it must accept as "facts of life" factors.

Chapter Five

APB BREACHES AND PROGRAM LIFE-CYCLES

The timing of deviations to baselines within a program's acquisition cycle was raised as an important concern of OUSD(A&T). To the extent that there are significant relationships—certain types of breaches occur more commonly at certain points in a program's acquisition cycle, or are associated with certain life-cycle events—acquisition managers may be better able to predict and respond to deviations from the baseline. Phase 2 of this research, documented in this chapter, explores the relationship between APB breaches and a program's acquisition life-cycle.

RESEARCH QUESTIONS

We address several inter-related questions regarding the relationship between the type and frequency of baseline breaches and acquisition program life-cycles.

- Is there a time-based pattern to the frequency of baseline breaches? Are breaches more likely to occur at certain points in a program's life-cycle or are they associated with specific life-cycle events? For instance, do relatively more breaches occur close to major decision points? Is there an association between breaches and budget cycles or early testing?
- Does the parameter breached (cost, schedule, performance) and the type of change (breach, revision, addition/deletion, improvement) vary systematically over a program's life-cycle? Do certain types of changes or breaches occur more frequently at certain times in the life-cycle or are they associated with specific

life-cycle events? For instance, do performance revisions occur after testing? Do revisions in general occur around milestone decisions? Are cost and schedule breaches associated with the budget cycle?

- Are certain factors that affect baseline breaches associated with specific life-cycle events or do they occur at points in a program's life-cycle related to program or technical maturity? For instance, do changes in specifications or mission occur around testing periods? Are quantity changes associated with the budget cycle?
- Are breaches that occur at certain times in a program's life-cycle, or associated with certain events, likely to be of relatively longer or shorter duration?

VARIABLES AND DATA

We constructed two types of variables relating to a program's acquisition life-cycle: a quantitative measure of program maturity and a qualitative measure of program life-cycle events. We also coded several additional variables related to the life-cycle event: the acquisition phase, the system of interest, and the relationship to the breach.

Program Maturity

The program maturity variable is a concept borrowed from past RAND research on the factors affecting weapon system cost growth. Program maturity, the time from a specified milestone to a specified event, was one of the few factors significantly affecting cost growth in weapon systems.[1] We developed seven different maturity indexes, defined as follows:

- *Years after Milestone 1*: Number of years between the baseline breach for a particular program and the Milestone 1 Defense Acquisition Board (DAB) decision.

[1]See J. A. Drezner et al., *An Analysis of Weapon System Cost Growth*, RAND, MR-291-AF, 1993.

- *Years after Milestone 2:* Number of years between the baseline breach and the Milestone 2 DAB decision to enter the engineering and manufacturing development phase.
- *Years after Milestone 3a:* Number of years between the baseline breach and the Milestone 3a DAB decision to begin low rate initial production.
- *Years after initial operational delivery:* Number of years between the baseline breach and the initial delivery of an operational system.
- *Years after IOT&E start:* Number of years between the baseline breach and the beginning of the initial operational testing phase.
- *Years after IOT&E completion:* Number of years between the baseline breach and the completion of the initial operational testing phase.
- *Months after approved APB:* Number of months between the baseline breach and the date at which the baseline being breached was approved.

Because the schedule and phase lengths of programs vary widely, each maturity index could potentially identify patterns unique to the program phase associated with the index's baseline. Dates for the APBs and breaches are from the databases developed to support the Phase 1 research described earlier. Milestone dates are taken from the Selected Acquisition Reports (SARs) for each program. Not every program has data for each of these variables, either because the data were not available or a milestone was not attained. Sometimes milestone dates had to be estimated because of differences in terminology among the services or other definitional issues. Rules for estimating milestone dates are the same as used in previous RAND studies.[2]

[2]See J. A. Drezner et al., *An Analysis of Weapon System Cost Growth*, RAND, MR-291-AF, 1993; Jeanne Jarvaise et al., *Defense System Cost Performance Database*, RAND, MR-625-OSD, 1996.

Life-Cycle Events

Life-cycle events are discrete activities or events that represent the dominant program office focus around the time of the breach. This is a nominal variable expressed as a taxonomy with the following categories:

- *Program review:* Formal program reviews, often focused on a specific decision. Includes DAB or service level equivalent meetings, DAES and DAB Readiness Review, Overarching Integrated Product Team (OIPT) review, and formal reviews of threat, requirements, and need.
- *Design reviews:* Formal technical reviews of program status, including Preliminary Design Review (PDR), Critical Design Review (CDR), and Production Readiness Review (PRR).
- *Source selection:* Formal process to select prime contractor for system or component after competition. Government only.
- *Test activity.* This includes any formal test program: contractor and government; development, operational, follow-on.
- *Other:* All other events/activities not categorized elsewhere. We include two important subcategories here: *routine contract* awards not associated with source selection decisions and *budget related decisions.*

The source selection category does not include routine contract awards in which a follow-on production option is exercised. A budget decision is not coded as "other" unless it is the dominant activity at the time of the breach.

Several issues are important here. First, life-cycle events are not necessarily the same as factors affecting the breach. In some cases, events and factors are the same (e.g., a major program review resulting in a program restructure that causes a schedule breach); in some cases, life-cycle events are independent (on-going test activities and Congressional budget cuts). Second, most program office activities—monitoring contractors, negotiating and awarding contracts, testing systems and subsystems, documenting program status, etc.—are continuous. In contrast, life-cycle events are discrete in time and place—a DAB meeting, source selection, a specific test failure. Third,

because the programs are varied, the only list of events that could be common to all programs in the database would be general. Finally, several events might take place concurrently against a background of the continuous activities. These issues significantly affect the analysis using the above taxonomy. To address the multiple event issue, we record each category separately, so a program might have as many as five events indicated.

Acquisition Phase

Definitions of the acquisition phases are based on the traditional acquisition decision milestones:

- *Pre EMD*: Stage of acquisition prior to decision to enter formal system development. Includes concept exploration and demonstration/validation phases. Bench-scale, laboratory, and prototype testing of systems or components may occur, usually to demonstrate technology or application. Prototype competitions leading to the selection of prime contractor for EMD included.
- *EMD*: Engineering and manufacturing development is the phase that starts at Milestone 2. This is the formal system development stage of the life-cycle. Both initial and subsequent development and operational testing occur in this phase. It may include competition leading to selection of the prime contractor for production.
- *Low rate initial production*: LRIP occurs after Milestone 3a or equivalent decision to begin production of the first units. The production rate is low but ramping up.
- *Production*: Post Milestone 3 full rate production decision. Rate production and deliveries are occurring.

We distinguish among three kinds of production: production of the original system, production of an upgraded system (block upgrades or major modification programs), and remanufacture of existing systems through a major modification program. The above scheme does not directly distinguish among these categories. Rather, a cross-tab analysis was performed using the "item of interest" variable to enable determination of whether the breach is associated with an on-going production of the original system configuration or

whether the breach is associated with on-going production of an upgraded or modified system.

Original vs. Modified Systems

The item of interest variable identifies whether it is the original system being breached or an upgrade.

- *System level*: The breach is associated with system level problems. This includes the original system, the original system with only slight changes from the first unit produced, and system integration issues.
- *System upgrade*: The breach is experienced by a major subsystem or component associated with a formal upgrade of the original system.

All upgrades and modifications are associated with the "upgrade" class. Our ability to accurately determine the correct coding, given the information in the SAR, may affect the analysis.

Event-Breach Relationship

The relationship of event to breach reflects our assessment as to whether the event being coded is related in some way to the breach. Four categories are relevant here:

- *None*: Life-cycle event clearly has no relationship to the breach.
- *Indirect*: Life-cycle event may have a relationship to the breach or the event indirectly affects the breach through one or more subsequent or related events.
- *Direct*: Life-cycle event clearly related to the breach.
- *Unknown*: Information is not adequate to make a determination about the relationship between the life-cycle event and the breach.

BASIC PATTERNS: TIMING AND EVENTS

Program Maturity and the Timing of Breaches

The timing of baseline breaches relative to a given program milestone is perhaps the most straightforward measure for observing whether acquisition life-cycles are associated with patterns of breaches. We constructed several maturity indexes based on this notion: each measures the time in years between a baseline breach and an acquisition program milestone for that program. The frequency distributions resulting from this exercise are shown in Figure 5.1.

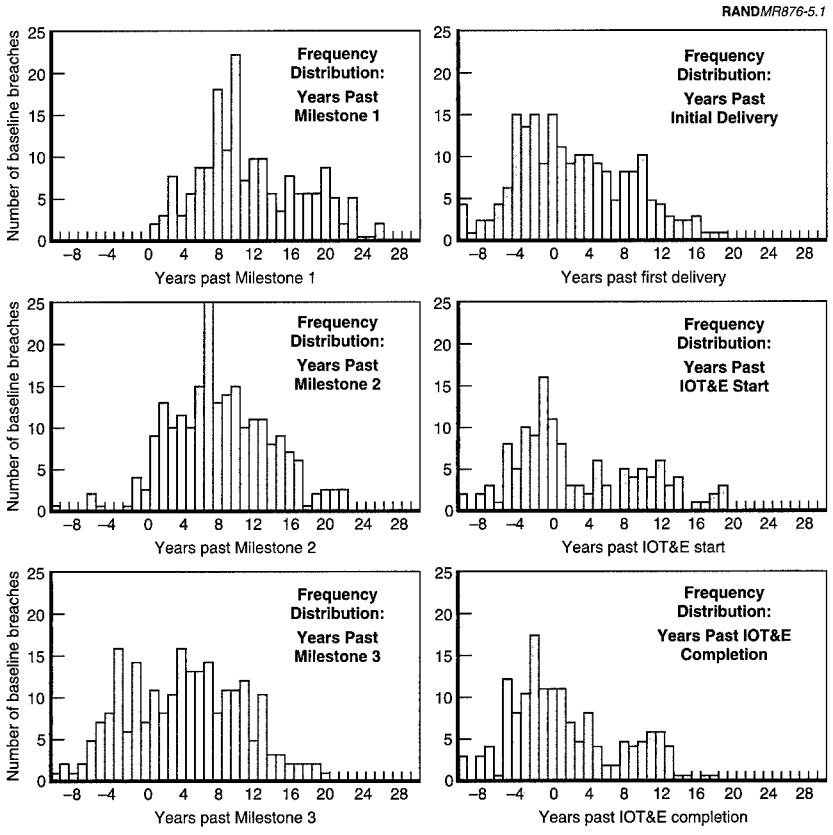


Figure 5.1—Number of Baseline Breaches vs. Program Maturity

All of the distributions shown share a similar pattern: they are slightly skewed toward the lower end of the scale. Most baseline breaches occur within about 10 years of major decision milestones. As a program matures—measured as time passing from a given milestone—baseline breaches become increasingly more likely to occur up to a certain point. As a program matures past this point, baseline breaches are relatively less common. That point is about 10 years past the milestone of interest. The most distinctive patterns occur when measuring maturity from Milestone 1, Milestone 2, and Initial Delivery.

Note that there are no breaches prior to Milestone 1 because APB reporting does not begin until after a program is approved for the demonstration/validation phase. Few breaches occur before Milestone 2, suggesting that the activities taking place during dem/val do not result in breaches as frequently. The majority of breaches occur after the EMD decision when system design, development, and test begin in earnest. For the most part, the number of programs experiencing breaches after the Milestone 3 production decision and Initial Delivery are relatively constant: about 10 each year for up to 10 years after these events. Note that the majority of these breaches occur prior to the start (and/or completion) of IOT&E.

Another interesting measure of the timing of APB breaches is the number of months between the approval date for an APB and the breach date. We would expect to see some significant passage of time, indicating that the resolution to the previous breach did in fact resolve a real problem. Figure 5.2 shows these data.

The vast majority (76 percent) of programs experienced a breach within 18 months of APB approval. This relatively short time span again suggests that breaches are common in acquisition program management. The implication is that a program with a 10 year EMD phase will likely experience 6 or 7 breaches during EMD. This projection corresponds reasonably well with the data presented in Chapter Three on the number of approved APBs (and thus breaches) each program has.

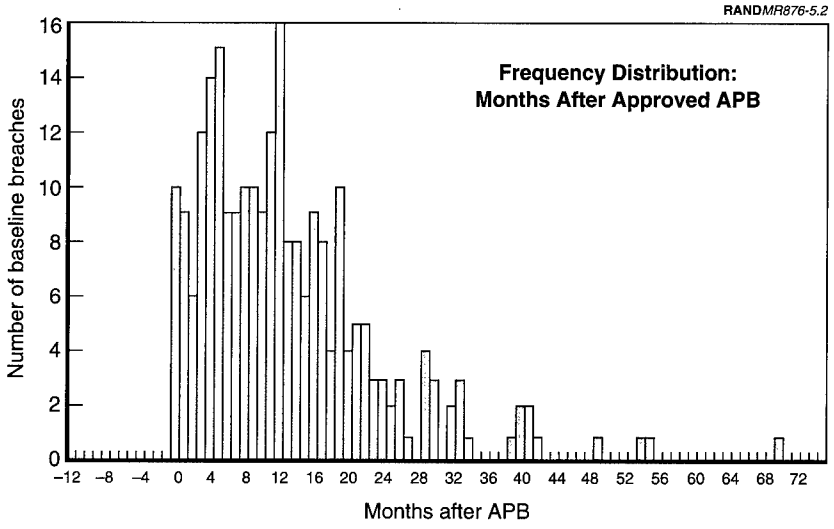


Figure 5.2—Timing of Breaches Relative to APB Approval

Frequency of Life-Cycle Events

Table 5.1 shows the frequency of program life-cycle events occurring around the time the programs in our database breached their baselines. More than one event could occur in a program at any given time.

Not surprisingly, over 80 percent of these programs were in some type of test activity at the time a breach was reported; some form of test activity is almost always being conducted.[3] This included both government and industry testing, as well as both developmental and operational testing at all program phases.

Program reviews and budget decisions occurred in conjunction with breaches with about the same frequency (23 percent). The specific type of test or program review or budget decision varied significantly

[3]This result suggests a need to improve this metric, perhaps by distinguishing among types of test activities.

Table 5.1

Frequency Count of Acquisition Life-Cycle Events at Time of Breach

Life-Cycle Event	Frequency	Percent of Total
Program review	53	23.7
Design review	12	5.4
Source selection	7	3.1
Test activity	184	82.1
Other	29	13.0
Contract award	20	8.9
Budget decision	51	22.8

NOTE: Denominator used in percent of total calculation is the total number of breaches for which we had sufficient information to code. Percentages do not sum to 100 because a breach may be associated with multiple events.

across programs. Even when the SARs provided information, the high variability did not lend itself to development of a useful taxonomy.

Table 5.2 summarizes the basic frequencies for the other variables in the analysis. As we would expect, most of the MDAPs are in production, so most of the breaches occurred during that phase. Similarly, 30 percent of the breaches occurred during EMD, reflecting the number of MDAPs in development. Most of the breaches were at the system level—that is, the original system was affected, as opposed to an upgrade or component. The number of breaches related to events that took place in the program at the time the breach occurred is about equal to the number that had no relationship to events. This surprising result may simply reflect the level of information available in the SARs concerning program events. Anecdotal evidence suggests a stronger relationship than documented here.

Table 5.3 cross-tabulates this information to identify relationships among life-cycle events, item of interest, and relationship of the event to the breach. Note that most testing and budget related events, at both the system and upgrade level, are equally split between a direct effect on the breach and no relationship at all. In contrast, most program reviews at the system level are associated with baseline breaches. This is the only strong relationship that can

Table 5.2

Frequency Count of Other Life-Cycle Event Variables

Variable	Frequency	Percent of Total
Acquisition Phase		
Pre EMD	9	4.0
EMD	67	29.9
LRIP	22	9.8
Production	122	54.5
Original vs. modification		
System level	157	70.1
Upgrade	67	29.9
Event-breach relationship		
No relation to breach	74	33.0
Direct effect	77	34.4
Indirect effect	22	9.8
Unknown	51	22.8

NOTE: Denominator used in percent of total calculation is the total number of breaches for which we had sufficient information to code.

be observed; it implies that when a program is reviewed a baseline breach often results. This is not necessarily a negative outcome: The purpose of program reviews is to make changes to a program so that it conforms better to DoD's needs in terms of cost (funding), schedule (timing), and performance (requirements).

Type of Change or Breach and Program Life-Cycle

One of our hypotheses was that program maturity would be related to the parameter that changed (cost, schedule, performance) and the type of change (breach, revision, addition/deletion, improvement). The notion was that certain types of changes and deviations might occur at certain points in the life-cycle of a program. Performance changes in the form of revisions or additions/deletions might occur relatively early in a program as developmental tests validate the initial trade-studies and modeling. Tables 5.4a and 5.4b provide information to assess this general hypothesis; for each of the seven maturity measures, the tables show the average value of the maturity index for each combination of change and deviation type. Few sig-

Table 5.3

Life-Cycle Events and Relationship to Breaches and Item of Interest

Life-Cycle Event	Direct Effect	Indirect Effect	No Effect	Unknown	Total
Test activity					
System level	50	9	49	22	130
Upgrade	17	8	13	16	54
Total	67	17	62	38	184
Program review					
System level	28	6	5	4	43
Upgrade	4	0	3	2	9
Total	32	6	8	6	52
Design review					
System level	2	0	2	2	6
Upgrade	0	1	2	3	6
Total	2	1	4	5	12
Source selection					
System level	3	1	2	1	7
Upgrade	0	0	0	0	0
Total	3	1	2	1	7
Contract award					
System level	6	0	9	3	18
Upgrade	0	0	1	1	2
Total	6	0	10	4	20
Budget decision					
System level	18	4	16	1	39
Upgrade	5	2	3	2	12
Total	23	6	19	3	51

nificant differences can be observed. The dominant result is a wide range and high standard deviation relative to the mean value.

Table 5.4a shows the results for the Years Past Milestone 1, Milestone 2, Milestone 3a, and Initial Delivery maturity indexes. For the Years Past Milestone 1 index, performance related deviations have very similar means and standard deviations. Cost revisions tend to occur somewhat earlier than cost breaches, and additions/deletions to schedule parameters occur somewhat later than schedule breaches or revisions. Nevertheless, few significant differences occur among the types of cost, schedule, and performance deviations. The Years Past Milestone 2 index shows almost identical patterns. There is a significant difference between the results for the two maturity indexes, however. For the index based on Milestone 2, the standard

Table 5.4a

Maturity and Breach Type

Parameter and Change	Years Past Milestone 1			Years Past Milestone 2			Years Past Milestone 3a			Years Past Initial Delivery		
	Avg	Std Dev	#obs	Avg	Std Dev	#obs	Avg	Std Dev	#obs	Avg	Std Dev	#obs
Cost												
Breach	11.7	5.07	62	8.3	5.62	72	4.0	6.53	79	2.3	6.76	66
Revision	8.6	5.01	16	6.2	4.61	21	2.8	4.94	19	0.9	4.91	18
Add/delete	10.4	4.42	3	7.8	2.22	4	3.9	4.47	4	–0.7	0.55	2
Improvement	8.4	7.82	5	6.4	8.13	5	3.5	7.79	6	3.6	8.10	4
Schedule												
Breach	9.6	4.61	68	6.4	4.75	84	2.4	5.83	87	0.2	5.57	79
Revision	10.5	6.15	14	8.1	6.40	13	4.5	7.48	16	3.3	7.13	14
Add/delete	15.6	5.22	14	11.4	5.10	17	7.8	5.78	16	7.4	5.11	13
Improvement	9.1		1	3.7		1	–1.1		1	–2.8		1
Performance												
Breach	11.1	5.98	16	8.1	6.68	18	4.7	7.00	19	3.1	8.58	13
Revision	10.4	5.98	23	7.1	6.00	23	3.7	7.10	23	1.6	6.99	24
Add/delete	11.8	5.95	15	7.3	6.06	17	4.0	7.00	17	2.8	6.45	15
Improvement	7.1		1	4.8	4.39	2	-2.8	.56	2	–5.3	1.09	2

Table 5.4b

Maturity and Breach Type

	Years Past IOT&E Start			Years Past IOT&E Complete			Months Past APB Approval		
Parameter and change	Avg	Std Dev	#obs	Avg	Std Dev	#obs	Avg	Std Dev	#obs
Cost									
Breach	2.4	7.56	43	1.6	6.52	53	13.2	11.45	84
Revision	1.3	6.41	10	–1.3	4.99	11	11.5	6.53	26
Addition/deletion	4.0	4.44	2			0	12.3	8.32	4
Improvement	2.7	8.29	5	2.8	7.44	6+	19.2	11.31	6
Schedule									
Breach	–0.2	6.20	47	-0.8	5.73	57	11.4	8.01	98
Revision	4.7	7.37	11	0.5	5.79	11	13.5	10.14	20
Addition/deletion	8.7	6.06	9	7.5	5.89	9	13.1	12.19	18
Improvement	–0.4		1	–0.5		1	5.3		1
Performance									
Breach	2.6	8.96	10	1.3	7.37	11	15.7	10.15	19
Revision	3.5	7.56	16	–1.5	5.16	13	13.0	9.20	37
Addition/deletion	2.5	9.04	11	1.8	7.79	13	14.1	9.30	19
Improvement	–3.5	2.33	2	–4.0	1.98	2	10.3	10.82	2

deviation is often of the same magnitude as the mean, and the range of values is quite large for all breach and deviation types. This suggests the very high variability across programs.

The general conclusion is that no strong relationships exist between the timing of a baseline breach relative to any particular acquisition milestone and the type of breach or deviation. The high variability observed across programs supports the notion that each program is affected by a unique set of internal and external factors and environmental characteristics.

Factors Affecting Breaches and Program Life-Cycles

In this part of the analysis we examine the relationship between program life-cycle events and the factors affecting program breaches identified in Chapter Four. Table 5.5 shows the results of this comparison. Funding or requirements changes are most often associated with program reviews and budget decisions. For the most part, however, there are no dominant or significant relationships. The number of breaches corresponding to particular mixes of program events and factors reflects the proportional representation (relative number) of life-cycle events and factors in the database. This result corresponds to the result discussed previously which showed that only about half of the events appear to be related to the breach in some way.

Table 5.5

Factors Affecting Breaches and Life-Cycle Events

Life-cycle Event/Item of Interest	Funding Related (n=81)	Technical Related (n=44)	Contractor Related (n=55)	Requirements Changes (n=62)	Program Redirection (n=70)
Program review	19	3	6	15	17
Design review	4	1	4	1	2
Test activity	57	35	40	38	51
Source selection	0	1	2	0	2
Contract award	7	5	8	6	5
Budget decision	27	5	8	11	11
System level	45	21	39	36	42
Upgrade	23	17	12	10	16

NOTE: Cell values are frequency (count) of number of breaches.

Table 5.6 shows the relationship between the seven maturity indexes and the factors affecting APB breaches. Few patterns emerge. Requirements changes are associated with program breaches relatively later in a program than other factors. This result is consistent across the different maturity indexes. With the exception of the years past Milestone 1 index, funding related factors tend to be associated with breaches somewhat earlier than other factors.

LIFE-CYCLES AND DURATION OF BREACH

The duration of APB breaches appears to be only slightly related to program maturity. Figure 5.3 plots the months a program remained in breach status against the program maturity measures used in this analysis. There is some clustering as well as a slight increase in duration. To some extent, baseline breaches occurring relatively early in a program tend to last a little longer than those occurring late in a program. This is not a statistically significant result, however. Given the results in Chapter Three concerning the duration of breaches in general (see Figures 3.6–3.9), this result is also not an artifact of the data: earlier breaches are longer not because they have more time in front of them to remain in breach.

Figure 5.4 plots the duration of a breach against the number of months from APB approval to the date of the breach. A relatively strong pattern can be observed here: breaches that occur a short passage of time after APB approval tend to be longer in duration. One possible explanation, consistent with the issue of recurring breaches within programs, is that the problem that caused the initial breach was not entirely resolved at the time the next APB was approved.

SUMMARY

The analysis presented here suggests few systematic relationships between program life-cycle events or program maturity and baseline breaches. This is true when considering the duration of breaches, the type of parameter that changed, the type of deviation, and the factors affecting the breach.

Table 5.6

Factors Affecting Breaches and Program Maturity

Life-cycle event	Funding Related	Technical Related	Contractor Related	Requirements Changes	Program Redirection
Years after Milestone 1	11.0 (5.32)	10.7 (6.00)	10.8 (4.84)	12.9 (5.77)	10.6 (5.85)
Years after Milestone 2	7.0 (5.44)	7.8 (5.27)	7.7 (4.47)	9.9 (5.15)	6.9 (5.94)
Years after Milestone 3a	2.4 (6.76)	4.0 (5.27)	4.2 (6.00)	5.6 (6.17)	2.9 (6.38)
Years after initial delivery	1.4 (6.58)	2.2 (5.65)	1.9 (5.56)	4.0 (5.57)	1.2 (6.89)
Years after IOT&E start	1.2 (6.85)	3.6 (6.90)	1.6 (6.53)	5.1 (6.89)	2.2 (8.04)
Years after IOT&E complete	0.5 (6.23)	1.8 (5.72)	0.8 (5.76)	3.4 (6.42)	–0.1 (5.92)
Months after APB approval	12.9 (8.91)	14.2 (8.01)	11.8 (7.30)	13.8 (12.4)	12.6 (8.07)

NOTE: Values in cells are average years/months for each variable. Standard deviations are shown in parentheses.

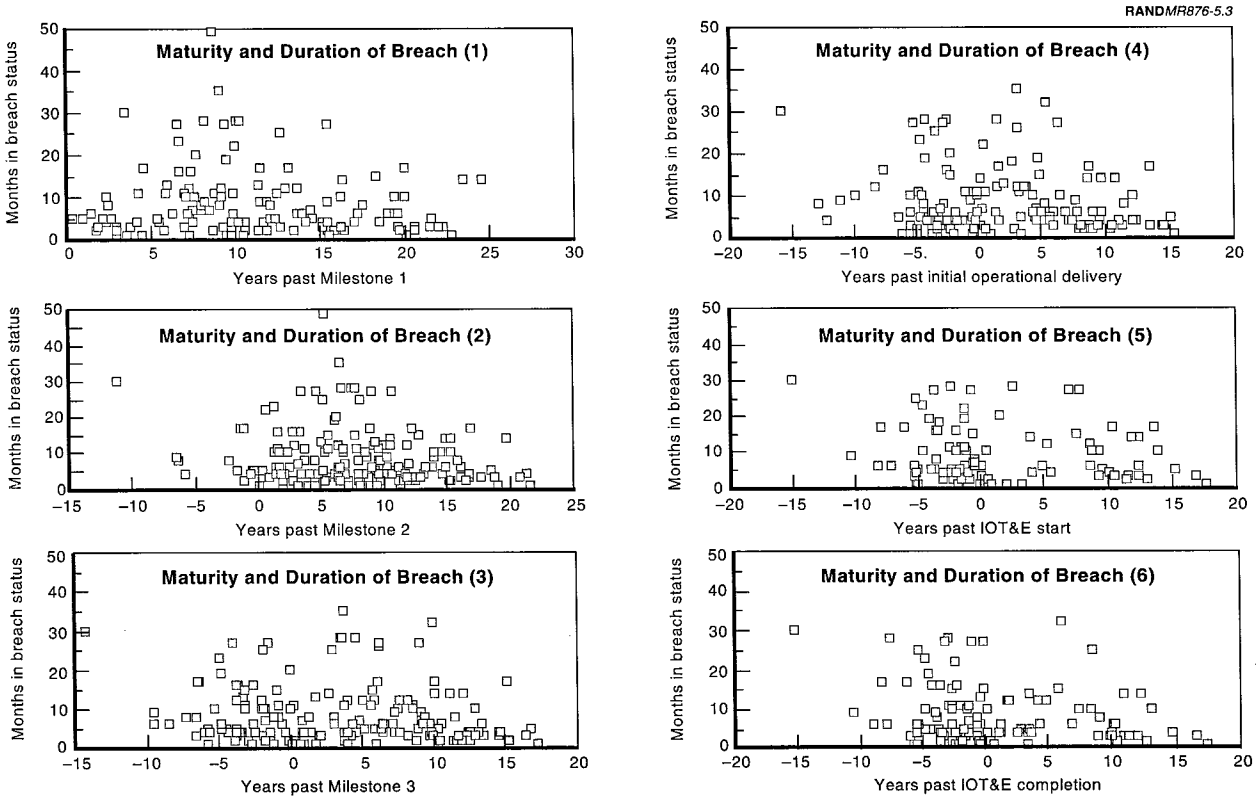


Figure 5.3—Maturity and Duration of Breach

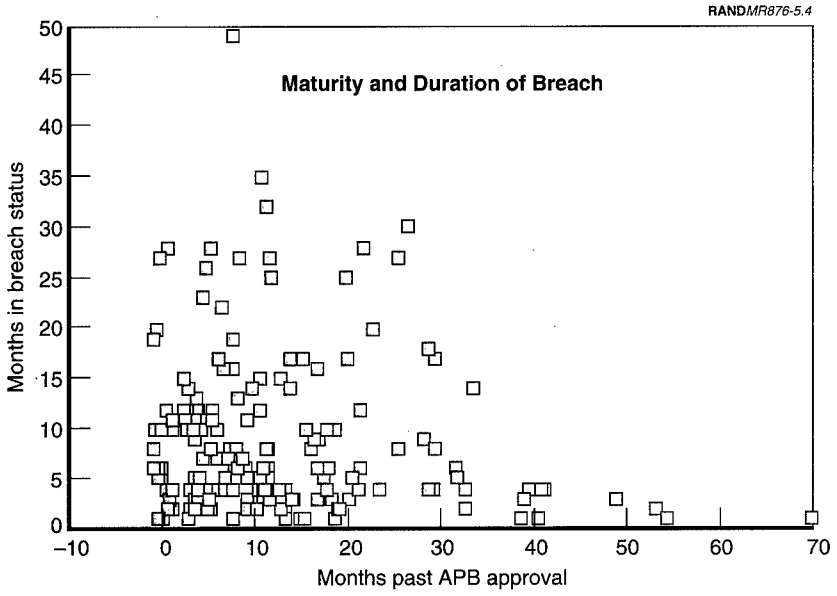


Figure 5.4—Duration of Breach and APB Approval

Although this result may reflect the quality and fidelity of the data used for this analysis, it is more likely that the unique characteristics of programs are the drivers behind the timing of APB breaches. Since each breach is associated with a unique set of programmatic and environmental factors, predicting the timing of such breaches remains uncertain.

Chapter Six

CONCLUSIONS

The establishment of APBs in 1988 was intended to enhance acquisition management by providing a process and documentation for reaching a consensus among acquisition decisionmakers about the key cost, schedule, and performance attributes of a program, as well as by providing a metric for re-evaluating the program when those attributes were at risk. The APB explicitly stated the management goals for a program, allowed tracking of progress against those goals, and provided for a process to review those goals as circumstances changed.

EVALUATING THE APB PROCESS

Our analyses suggest that most programs will have at least one breach of their baselines at some point in their life-cycles. This should be expected at the start of any program and should not be interpreted negatively. Given the complexities of both the weapons systems being developed and the acquisition process itself, there needs to be enough flexibility to adjust a program as technical knowledge is gained and as the economic and security environment changes. The APB process provides acquisition decisionmakers with a necessary management tool for reviewing programs and documenting changes as events warrant.

It is difficult to use the frequency of baseline breaches or the duration of those breaches as measures of overall DoD acquisition program success. On average, both the frequency and the duration of breaches have declined over the last several years, even after adjusting for the number of active programs in development or production.

The drivers of these trends are not clear however, suggesting that the trends should be interpreted cautiously. Frequent breaches of long duration may reflect that the acquisition process is performing as intended—identifying programs with problems and then providing for their resolution.[1]

Our analysis could detect no dominant factor affecting breaches. Nor could we identify any time or event-based patterns to when breaches occur in a program's life-cycle. Further, multiple factors affecting a breach and multiple programmatic events associated with the breach are common. Each program has unique characteristics, both in terms of technology and the political and economic aspects of the acquisition process, and these characteristics are the real determinants of program performance.

Not all baseline breaches are equivalent. Even though the thresholds for breaches are the same across programs for the programs in our database, the relative importance of the breach, the relative importance of the parameter being breached, and the magnitude of the change are all different.

RECOMMENDATIONS

Based on the results of our analysis and our observation of how the APB process actually works in practice, we have two related sets of recommendations for enhancing the usefulness of the APB as a management tool.

Tailoring the Parameters and Thresholds

First, careful tailoring of the parameters included in the APB, the thresholds associated with those parameters, and the responses to baseline breaches should be implemented to the fullest extent possible. Current regulations allow for, even encourage tailoring both parameters and thresholds to the unique characteristics of the pro-

[1]An interesting area for future analysis concerns the impact of risk on both the frequency and duration of breaches. While we might expect a relatively higher-risk program to have more breaches of greater length (more difficult to resolve), a more realistic assessment of program risks at the time the baseline is established might have an opposite effect. Additional data would need to be collected to test these hypotheses.

gram. We believe that this is an appropriate way to reflect the relative importance and risk in each program. We do not believe that standard thresholds for classes of weapon systems (e.g., aircraft, ships, etc.) can be usefully developed because of the unique characteristics of each program, independent of system type. OSD acquisition officials and the program office could negotiate the parameters to include and their associated thresholds.

Along these lines, we believe that parameters included in program baselines should be limited to truly critical ones: a breach in a parameter means that a program review is justified. In practice, this means, for instance, that all schedule milestones and events do not need to be listed; only those critical to meeting operational needs (e.g., IOC) or requiring major funding increments (e.g., start of EMD or production) might be necessary. Another suggestion is to define parameters that are tailored to each phase and better reflect actual risk and development events, as opposed to reflected administrative processes. Given that the risk might change as a program transitions to subsequent phases (for a variety of reasons), the parameter set included in the APB could be different for each phase.

Tailoring has the further advantage of making subsequent breaches equivalent in importance across programs, since thresholds should reflect the risk preferences of decisionmakers and those preferences can be consistently applied across programs. Equivalence in importance may imply high thresholds for low cost, low risk, lower priority programs or very low thresholds for high cost, high visibility, high priority programs. Equivalence as used here refers to how criteria are applied when setting parameter thresholds, not the amount of management attention each program receives.

The critical implementation challenge here is to develop a set of criteria for establishing parameters to include and the thresholds associated with those parameters that can be consistently applied across programs. Parameters to include should be limited to those that are necessary to define the key technical and operational characteristics of the system, schedule milestones reflecting actual development progress, and cost and quantity metrics. The thresholds for these parameters should reflect the risk preferences and sensitivities of the key acquisition decisionmakers associated with the program, and

should be set at a level that warrants high level program review and re-evaluation.

Making Distinctions Among Breaches and Their Causes

Our second recommendation is to make several important substantive and semantic distinctions among breaches and the causes of those breaches. For the reasons explained above, breaches should not be interpreted as adversely reflecting the quality of program management. The current effect of the negative connotations associated with breaches includes delayed reporting (and thus delayed awareness by OSD acquisition officials of potential problems) and vague information about the causes of the breach. Negative connotations should be removed, thus encouraging faster breach reporting and more thorough documentation of the causes (factors).

Similarly, a distinction should be made between factors that DoD has some ability to influence, and those that are entirely external to DoD's acquisition management processes. Figure 6.1 provides a notional illustration of the relative distribution of internal and external factors affecting breaches, based on the data presented in Chapter Four. Based on our knowledge of the factors included in this analysis, we categorized the second-order factors as either internal or external to DoD, and then aggregated their relative frequencies to the first-order factor taxonomy. Although this rough estimate is meant to provide a notional illustration of a useful exercise that should be conducted in more detail, we believe that slightly over half of the breaches are caused by factors or events that DoD has some ability to influence. Relatively more attention to these breaches and the factors that cause them would enhance the usefulness of the APB process.

The acquisition program baselining process provides substantial opportunity for improved communication between service and program office officials and OSD acquisition managers and decision-makers. The APB process generates good information; focusing attention on collecting, organizing, and disseminating this information could significantly enhance the usefulness of the APB process for acquisition management.

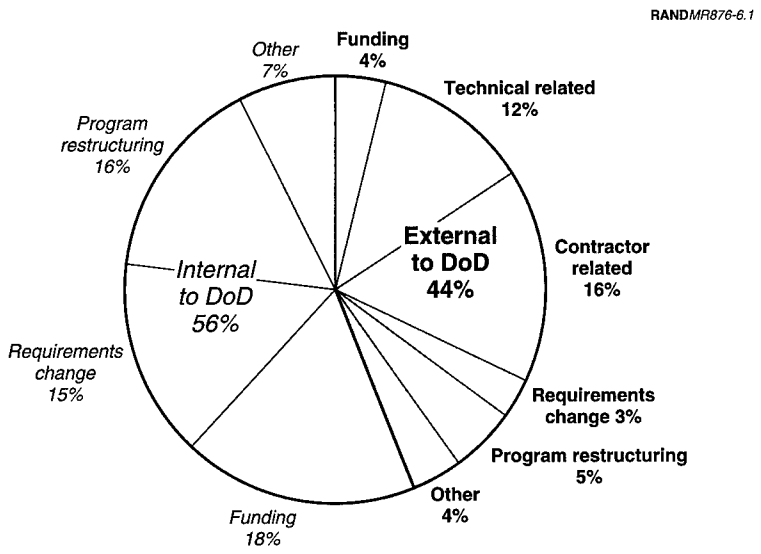


Figure 6.1—Notional Distribution of Internal and External Factors Affecting Breaches

Preceding Page Blank

Appendix

THE ANALYTICAL TOOL

The first phase of the analysis described in this report was supported by several spreadsheets. These spreadsheets were given to OUSD(A&T)API/ASM to support continued analysis of these data. This appendix provides a brief overview of each of the spreadsheets. The spreadsheets serve two purposes. First, they provide a means to collect and store data on the number of baselines; the number, type, and duration of baseline breaches; and the factors that affect the baseline breaches. Second, they produce summary analyses of the data, in both tabular and graphical form. The spreadsheets are in Microsoft Excel, version 5.0 for Windows. Users should be familiar with Excel before using the spreadsheets.

The data are in three spreadsheet workbooks. The first workbook, BREACH.XLS, stores and summarizes the data on the number and duration of breaches. The second workbook, APBDATA.XLS, contains data on the baselines themselves, including the date of the baseline and the type of revisions made to the baseline, if any. The third workbook, FACTORS.XLS, contains the data on the factors that affect baseline breaches. A fourth sheet, APB_TOOL.XLS, provides access to each workbook.

The file BREACH.XLS tracks the number of programs in breach and the duration of the breaches. It reports whether or not a program is in breach in a given month, and how long it has been in breach at that point. It calculates the total number of programs in breach in a given month, as well as several measures of the average duration of baseline breaches. It also keeps track of the components of monthly

turnover in program breaches. These calculations are carried out in several spreadsheets, which are described in Table A.1.

The basic data for all the calculations carried out by BREACH.XLS are entered in the first sheet, Monthly Breaches. The format of this sheet is described in Table A.2.

BREACH.XLS also contains a series of charts that summarize the data. These charts are stored as separate sheets in the workbook. The charts in the workbook include:

- The total number of breaches and the number of breaches as a percentage of MDAPs, by month, for all of DoD and by service.
- The total number of cost, schedule, and performance breaches.
- The average duration of each baseline breach when the breach is resolved, for all of DoD and by service.

Table A.1

Contents of Workbook File BREACH.XLS

Spreadsheet Name	Contents
Monthly Breaches	Contains raw data, by weapon system and baseline.
Avg Duration	Stores length of time each baseline remained in breach. These data are used to calculate the average duration of program breaches.
Time in Breach	Shows number of months each program is in breach by year, and for the period covered by the spreadsheet. These data are based on data in the Monthly Breaches sheet, and are used to calculate frequency distributions of the duration of breaches.
Turnover	Calculates the components of monthly turnover: new breaches, resolved breaches, breaches carried over from one month to the next, and total number of programs in breach.
MDAP	List of Major Defense Acquisition Programs, for 1992 on, by service. Also indicates if MDAP has an approved baseline, and if it is an ACAT I C or D.

Table A.2

Layout of Monthly Breaches Sheet in Workbook BREACH.XLS

Column	Contents of Column
A	Name of weapon system
B	Service (Army, Navy, Air Force, DoD Agencies)
C	APB Date
D	ACAT I category (A or C)
E	Date baseline breached for first time
F–H	Type of parameter that breached: cost, schedule, performance
I–BG	Months of the year, starting April 1992, and ending June 1996. These columns indicate whether a program is in breach in a given month. If in breach, indicates number of months it has been in breach by that time. (Uses a formula, adding 1 to the content of the previous month's entry.)
BH	Marks end of data. To add a new month, click on this column and insert a new column. This ensures that references in workbook remain valid.
BI	Number of months each program on list was in breach in 1992
BJ	Number of months each program on list was in breach in 1993
BK	Number of months each program on list was in breach in 1994
BL	Number of months each program on list was in breach in 1995
BM	Number of months each program on list was in breach in 1996
BN	Number of months each program on list was in breach from 1992 through June 1996
BO	Number of months each program on list was in breach in from April 1992 through June 1996
BP	Notes on each baseline
BQ–BR	Codes used to sort the data

- Number of new breaches, breaches resolved, breaches carried over, and total number of breaches, by month, for all of DoD and by service, by raw counts and as a percentage of MDAPs.
- Histograms of the frequency distribution of the duration of baseline breaches.

The workbook APBDATA.XLS keeps track of each program's baselines. It shows the date of each baseline, and, for revised baselines, the type of change that was made. It indicates whether the change was to the cost, schedule, or performance portion of the baseline, and distinguishes among four types of changes: (1) breaches to thresholds, (2) revisions that do not breach baseline thresholds, (3) additions and deletions of parameters (no original thresholds exceeded), and (4) improvements to baseline targets. The data on each baseline are stored in the sheet labeled "Data"; the sheet "Summary" summarizes the number and type of baseline changes by service, type of parameter affected, and type of change to the baseline. Table A.3 describes the layout of the Data sheet of the APBDATA.XLS Workbook.

The final file contains a taxonomy of the causes of breaches of acquisition program baselines. It codifies past breaches according to

Table A.3

Layout of Data Sheet in Workbook APBDATA.XLS

Column	Contents of Column
A	Weapon system name
B	Service (Army, Navy, Air Force, DoD Agencies)
C	Date of baseline
D	Type of baseline
E	Number of baseline
F	Indicates whether cost portion of baseline was changed, and type of change
G	Indicates whether schedule portion of baseline was changed, and type of change
H	Indicates whether performance portion of baseline was changed, and type of change
I	Indicates the phase program was in when breach occurred

the reason given for the breach identified in program deviation reports. It contains three sheets. The sheet Rules contains the rules applied in coding breaches by factor. It also defines each factor. The factors for each baseline breach are coded in the spreadsheets Factors. The factors are summarized in the sheet Summary. The format of the sheet Factors is described in Table A.4.

Table A.4

Layout of Factors Sheet in Workbook FACTORS.XLS

Column	Contents of Column
A	Name of the weapon system
B	Military service
C	Date of baseline
D	Date of the program deviation report
E	Type of breach (cost, schedule, or performance)
F–J	The five funding related factors
K–M	The three technical related factors
N–R	The five contractor related factors
S–U	The three requirements change factors
V–Y	The four program restructuring factors
Z–AA	Two other, miscellaneous factors
AB–AG	Summary of the six higher level factors